VISIT…

© The McGraw–Hill Companies, 2004

Preface

Discrete mathematics, the study of finite systems, has become increasingly important as the computer age has advanced. The digital computer is basically a finite structure, and many of its properties can be understood and interpreted within the framework of finite mathematical systems. This book, in presenting the more essential material, may be used as a textbook for a formal course in discrete mathematics or as a supplement to all current texts.

The first three chapters cover the standard material on sets, relations, and functions and algorithms. Next come chapters on logic, vectors and matrices, counting, and probability. We than have three chapters on graph theory: graphs, directed graphs, and binary trees. Finally there are individual chapters on properties of the integers, algebraic systems, languages and machines, ordered sets and lattices, and Boolean algebra. The chapter on functions and algorithms includes a discussion of cardinality and countable sets, and complexity. The chapters on graph theory include discussions on planarity, traversability, minimal paths, and Warshall's and Huffman's algorithms. The chapter on languages and machines includes regular expressions, automata, and Turing machines and computable functions. We emphasize that the chapters have been written so that the order can be changed without difficulty and without loss of continuity.

This second edition of *Discrete Mathmatics* covers much more material and in greater depth than the first edition. The topics of probability, regular expressions and regular sets, binary trees, cardinality, complexity, and Turing machines and computable functions did not appear in the first edition or were only mentioned. This new material reflects the fact that discrete mathematics now is mainly a one-year course rather than a one-semester course.

Each chapter begins with a clear statement of pertinent definition, principles, and theorems with illustrative and other descriptive material. This is followed by sets of solved and supplementary problems. The solved problems serve to illustrate and amplify the material, and also include proofs of theorems. The supplementary problems furnish a complete review of the material in the chapter. More material has been included than can be covered in most first courses. This has been done to make the book more flexible, to provide a more useful book of reference, and to stimulate further interest in the topics.

Finally, we wish to thank the staff of the McGraw-Hill Schaum's Outline Series, especially Arthur Biderman and Maureen Walker, for their unfailing cooperation.

Seymour Lipschutz
Marc Lars Lipson

© The McGraw–Hill Companies, 2004

Chapter 1

Set Theory

1.1 INTRODUCTION

The concept of a *set* appears in all mathematics. This chapter introduces the notation and terminology of set theory which is basic and used throughout the text.

Though logic is formally treated in Chapter 4, we introduce Venn diagram representation of sets here, and we show how it can be applied to logical arguments. The relation between set theory and logic will be further explored when we discuss Boolean algebra in Chapter 15.

This chapter closes with the formal definition of mathematical induction, with examples.

1.2 SETS AND ELEMENTS

A *set* may be viewed as a collection of objects, the *elements* or *members* of the set. We ordinarily use capital letters, A, B, X, Y, ..., to denote sets, and lowercase letters, a, b, x, y, ..., to denote elements of sets. The statement "p is an element of A", or, equivalently, "p belongs to A", is written

$$p \in A$$

The statement that p is not an element of A, that is, the negation of $p \in A$, is written

$$p \notin A$$

The fact that a set is completely determined when its members are specified is formally stated as the principle of extension.

Principle of Extension: Two sets A and B are equal if and only if they have the same members.

As usual, we write $A = B$ if the sets A and B are equal, and we write $A \neq B$ if the sets are not equal.

Specifying Sets

There are essentially two ways to specify a particular set. One way, if possible, is to list its members. For example,

$$A = \{\text{a}, \text{e}, \text{i}, \text{o}, \text{u}\}$$

denotes the set A whose elements are the letters a, e, i, o, u. Note that the elements are separated by commas and enclosed in braces { }. The second way is to state those properties which characterized the elements in the set. For example,

$$B = \{x\text{: } x \text{ is an even integer, } x > 0\}$$

which reads "B is the set of x such that x is an even integer and x is greater than 0", denotes the set B whose elements are the positive integers. A letter, usually x, is used to denote a typical member of the set; the colon is read as "such that" and the comma as "and".

EXAMPLE 1.1

(*a*) The set A above can also be written as

$$A = \{x\text{: } x \text{ is a letter in the English alphabet, } x \text{ is a vowel}\}$$

Observe that $\text{b} \notin A$, $\text{e} \in A$, and $\text{p} \notin A$.

(*b*) We could not list all the elements of the above set B although frequently we specify the set by writing

$$B = \{2, 4, 6, \ldots\}$$

where we assume that everyone knows what we mean. Observe that $8 \in B$ but $-7 \notin B$.

(*c*) Let $E = \{x: x^2 - 3x + 2 = 0\}$. In other words, E consists of those numbers which are solutions of the equation $x^2 - 3x + 2 = 0$, sometimes called the *solution set* of the given equation. Since the solutions of the equation are 1 and 2, we could also write $E = \{1, 2\}$.

(*d*) Let $E = \{x: x^2 - 3x + 2 = 0\}$, $F = \{2, 1\}$ and $G = \{1, 2, 2, 1, \frac{6}{3}\}$. Then $E = F = G$. Observe that a set does not depend on the way in which its elements are displayed. A set remains the same if its elements are repeated or rearranged.

Some sets will occur very often in the text and so we use special symbols for them. Unless otherwise specified, we will let

$$\begin{aligned}
\mathbf{N} &= \text{the set of positive integers: } 1, 2, 3, \ldots \\
\mathbf{Z} &= \text{the set of integers: } \ldots, -2, -1, 0, 1, 2, \ldots \\
\mathbf{Q} &= \text{the set of rational numbers} \\
\mathbf{R} &= \text{the set of real numbers} \\
\mathbf{C} &= \text{the set of complex numbers}
\end{aligned}$$

Even if we can list the elements of a set, it may not be practical to do so. For example, we would not list the members of the set of people born in the world during the year 1976 although theoretically it is possible to compile such a list. That is, we describe a set by listing its elements only if the set contains a few elements; otherwise we describe a set by the property which characterizes its elements.

The fact that we can describe a set in terms of a property is formally stated as the *principle of abstraction*.

Principle of Abstraction: Given any set U and any property P, there is a set A such that the elements of A are exactly those members of U which have the property P.

1.3 UNIVERSAL SET AND EMPTY SET

In any application of the theory of sets, the members of all sets under investigation usually belong to some fixed large set called the *universal set*. For example, in plane geometry, the universal set consists of all the points in the plane, and in human population studies the universal set consists of all the people in the world. We will let the symbol

$$U$$

denote the universal set unless otherwise stated or implied.

For a given set U and a property P, there may not be any elements of U which have property P. For example, the set

$$S = \{x: x \text{ is a positive integer}, x^2 = 3\}$$

has no elements since no positive integer has the required property.

The set with no elements is called the *empty set* or *null set* and is denoted by

$$\varnothing$$

There is only one empty set. That is, if S and T are both empty, then $S = T$ since they have exactly the same elements, namely, none.

1.4 SUBSETS

If every element in a set A is also an element of a set B, then A is called a *subset* of B. We also say that A is *contained* in B or that B *contains* A. This relationship is written

$$A \subseteq B \qquad \text{or} \qquad B \supseteq A$$

If A is not a subset of B, i.e., if at least one element of A does not belong to B, we write $A \nsubseteq B$ or $B \not\supseteq A$.

EXAMPLE 1.2

(*a*) Consider the sets

$$A = \{1, 3, 4, 5, 8, 9\} \qquad B = \{1, 2, 3, 5, 7\} \qquad C = \{1, 5\}$$

Then $C \subseteq A$ and $C \subseteq B$ since 1 and 5, the elements of C, are also members of A and B. But $B \nsubseteq A$ since some of its elements, e.g., 2 and 7, do not belong to A. Furthermore, since the elements of A, B, and C must also belong to the universal set U, we have that U must at least contain the set $\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$.

(*b*) Let $\mathbf{N}$, $\mathbf{Z}$, $\mathbf{Q}$, and $\mathbf{R}$ be defined as in Section 1.2. Then

$$\mathbf{N} \subseteq \mathbf{Z} \subseteq \mathbf{Q} \subseteq \mathbf{R}$$

(*c*) The set $E = \{2, 4, 6\}$ is a subset of the set $F = \{6, 2, 4\}$, since each number 2, 4, and 6 belonging to E also belongs to F. In fact, $E = F$. In a similar manner it can be shown that every set is a subset of itself.

The following properties of sets should be noted:

(i) Every set A is a subset of the universal set U since, by definition, all the elements of A belong to U. Also the empty set $\varnothing$ is a subset of A.

(ii) Every set A is a subset of itself since, trivially, the elements of A belong to A.

(iii) If every element of A belongs to a set B, and every element of B belongs to a set C, then clearly every element of A belongs to C. In other words, if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

(iv) If $A \subseteq B$ and $B \subseteq A$, then A and B have the same elements, i.e., $A = B$. Conversely, if $A = B$ then $A \subseteq B$ and $B \subseteq A$ since every set is a subset of itself.

We state these results formally.

Theorem 1.1: (i) For any set A, we have $\varnothing \subseteq A \subseteq U$.
(ii) For any set A, we have $A \subseteq A$.
(iii) If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.
(iv) $A = B$ if and only if $A \subseteq B$ and $B \subseteq A$.

If $A \subseteq B$, then it is still possible that $A = B$. When $A \subseteq B$ but $A \neq B$, we say A is a *proper subset* of B. We will write $A \subset B$ when A is a proper subset of B. For example, suppose

$$A = \{1, 3\} \qquad B = \{1, 2, 3\}, \qquad C = \{1, 3, 2\}$$

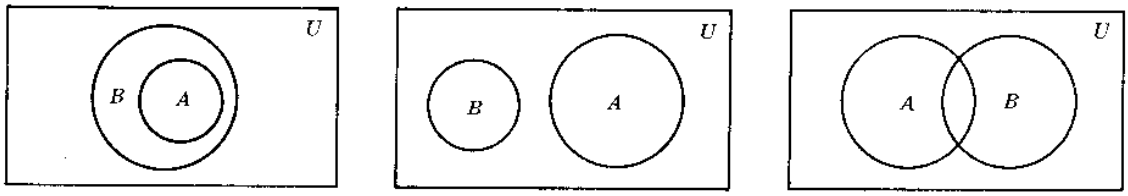
Then A and B are both subsets of C; but A is a proper subset of C, whereas B is not a proper subset of C since $B = C$.

1.5 VENN DIAGRAMS

A Venn diagram is a pictoral representation of sets in which sets are represented by enclosed areas in the plane.

The universal set U is represented by the interior of a rectangle, and the other sets are represented by disks lying within the rectangle. If $A \subseteq B$, then the disk representing A will be entirely within the disk representing B as in Fig. 1-1(*a*). If A and B are disjoint, i.e., if they have no elements in common, then the disk representing A will be separated from the disk representing B as in Fig. 1-1(*b*).

However, if A and B are two arbitrary sets, it is possible that some objects are in A but not in B, some are in B but not in A, some are in both A and B, and some are in neither A nor B; hence in general we represent A and B as in Fig. 1-1(*c*).



(a) $A \subset B$ (b) A and B are disjoint (c)

Fig. 1-1

Arguments and Venn Diagrams

Many verbal statements are essentially statements about sets and can therefore be described by Venn diagrams.

Hence Venn diagrams can sometimes be used to determine whether or not an argument is valid. Consider the following example.

EXAMPLE 1.3 Show that the following argument (adapted from a book on logic by Lewis Carroll, the author of *Alice in Wonderland*) is valid:

S_1: My saucepans are the only things I have that are made of tin.
S_2: I find all your presents very useful.
S_3: None of my saucepans is of the slightest use.

S: Your presents to me are not made of tin.

(The statements S_1, S_2, and S_3 above the horizontal line denote the assumptions, and the statement S below the line denotes the conclusion. The argument is valid if the conclusion S follows logically from the assumptions S_1, S_2, and S_3.)

By S_1 the tin objects are contained in the set of saucepans and by S_3 the set of saucepans and the set of useful things are disjoint: hence draw the Venn diagram of Fig. 1-2.

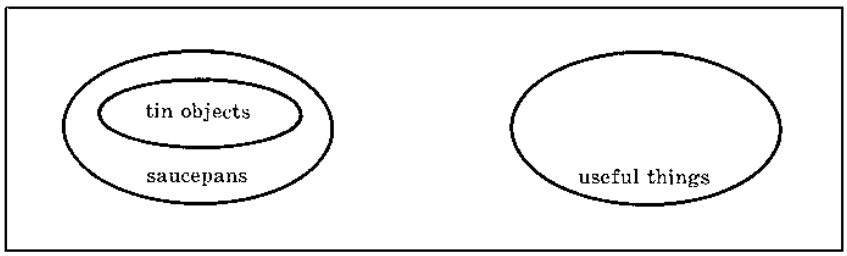


Fig. 1-2

By S_2 the set of "your presents" is a subset of the set of useful things; hence draw Fig. 1-3.

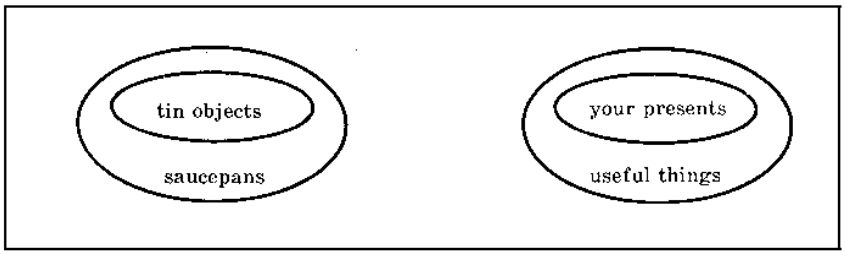


Fig. 1-3

The conclusion is clearly valid by the above Venn diagram because the set of "your presents" is disjoint from the set of tin objects.

1.6 SET OPERATIONS

This section introduces a number of important operations on sets.

Union and Intersection

The *union* of two sets A and B, denoted by $A \cup B$, is the set of all elements which belong to A or to B; that is,

$$A \cup B = \{x\colon x \in A \text{ or } x \in B\}$$

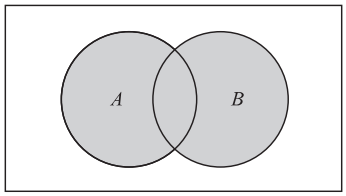
Here "or" is used in the sense of and/or. Figure 1-4(a) is a Venn diagram in which $A \cup B$ is shaded.

The *intersection* of two sets A and B, denoted by $A \cap B$, is the set of elements which belong to both A and B; that is,

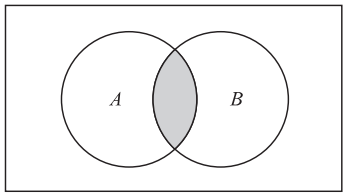
$$A \cap B = \{x\colon x \in A \text{ and } x \in B\}$$

Figure 1-4(b) is a Venn diagram in which $A \cap B$ is shaded.

If $A \cap B = \varnothing$, that is, if A and B do not have any elements in common, then A and B are said to be *disjoint* or *nonintersecting*.



(a) $A \cup B$ is shaded



(b) $A \cap B$ is shaded

Fig. 1-4

EXAMPLE 1.4

(a) Let $A = \{1, 2, 3, 4\}$, $B = \{3, 4, 5, 6, 7\}$, $C = \{2, 3, 5, 7\}$. Then

$$A \cup B = \{1, 2, 3, 4, 5, 6, 7\} \qquad A \cap B = \{3, 4\}$$
$$A \cup C = \{1, 2, 3, 4, 5, 7\} \qquad A \cap C = \{2, 3\}$$

(*b*) Let M denote the set of male students in a university C, and let F denote the set of female students in C. Then

$$M \cup F = C$$

since each student in C belongs to either M or F. On the other hand,

$$M \cap F = \varnothing$$

since no student belongs to both M and F.

The operation of set inclusion is closely related to the operations of union and intersection, as shown by the following theorem.

Theorem 1.2: The following are equivalent: $A \subseteq B$, $A \cap B = A$, and $A \cup B = B$.

Note: This theorem is proved in Problem 1.27. Other conditions equivalent to $A \subseteq B$ are given in Problem 1.37.

Complements

Recall that all sets under consideration at a particular time are subsets of a fixed universal set U. The *absolute complement* or, simply, *complement* of a set A, denoted by A^c, is the set of elements which belong to U but which do not belong to A; that is,

$$A^c = \{x: x \in U, x \notin A\}$$

Some texts denote the complement of A by A' or $\bar{A}$. Figure 1-5(*a*) is a Venn diagram in which A^c is shaded.

The *relative complement* of a set B with respect to a set A or, simply, the *difference* of A and B, denoted by $A\backslash B$, is the set of elements which belong to A but which do not belong to B; that is

$$A\backslash B = \{x: x \in A, x \notin B\}$$

The set $A\backslash B$ is read "A minus B". Many texts denote $A\backslash B$ by $A - B$ or $A \sim B$. Figure 1-5(*b*) is a Venn diagram in which $A\backslash B$ is shaded.

(*a*) A^c is shaded (*b*) $A\backslash B$ is shaded

Fig. 1-5

EXAMPLE 1.5 Suppose $U = \mathbf{N} = \{1, 2, 3, \ldots\}$, the positive integers, is the universal set. Let

$$A = \{1, 2, 3, 4, \}, \qquad B = \{3, 4, 5, 6, 7\}, \qquad C = \{6, 7, 8, 9\}$$

and let $E = \{2, 4, 6, 8, \ldots\}$, the even integers. Then

$$A^c = \{5, 6, 7, 8, \ldots\}, \qquad B^c = \{1, 2, 8, 9, 10, \ldots\}, \qquad C^c = \{1, 2, 3, 4, 5, 10, 11, \ldots\}$$

and

$$A\backslash B = \{1, 2\}, \qquad B\backslash C = \{3, 4, 5\}, \qquad B\backslash A = \{5, 6, 7\}, \qquad C\backslash E = \{7, 9\}$$

Also, $E^c = \{1, 3, 5, \ldots\}$, the odd integers.

Fundamental Products

Consider n distinct sets $A_1, A_2, \ldots, A_n$. A *fundamental product* of the sets is a set of the form

$$A_1^* \cap A_2^* \cap \cdots \cap A_n^*$$

where A_i^* is either A_i or A_i^c. We note that (1) there are 2^n such fundamental products, (2) any two such fundamental products are disjoint, and (3) the universal set U is the union of all the fundamental products (Problem 1.64). There is a geometrical description of these sets which is illustrated below.

EXAMPLE 1.6 Consider three sets A, B, and C. The following lists the eight fundamental products of the three sets:

$$P_1 = A \cap B \cap C, \quad P_3 = A \cap B^c \cap C, \quad P_5 = A^c \cap B \cap C, \quad P_7 = A^c \cap B^c \cap C$$
$$P_2 = A \cap B \cap C^c \quad P_4 = A \cap B^c \cap C^c, \quad P_6 = A^c \cap B \cap C^c \quad P_8 = A^c \cap B^c \cap C^c$$

These eight products correspond precisely to the eight disjoint regions in the Venn diagram of sets A, B, C in Fig. 1-6 as indicated by the labeling of the regions.

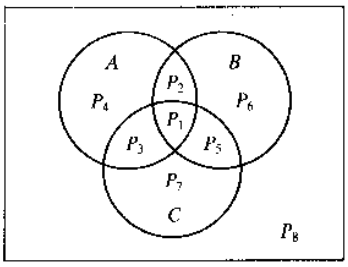
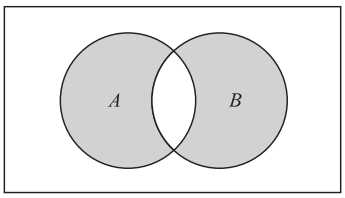


Fig. 1-6



$A \oplus B$ is shaded

Fig. 1-7

Symmetric Difference

The *symmetric difference* of sets A and B, denoted by $A \oplus B$, consists of those elements which belong to A or B but not to both; that is,

$$A \oplus B = (A \cup B) \backslash (A \cap B)$$

One can also show (Problem 1.18) that

$$A \oplus B = (A \backslash B) \cup (B \backslash A)$$

For example, suppose $A = \{1, 2, 3, 4, 5, 6\}$ and $B = \{4, 5, 6, 7, 8, 9\}$. Then

$$A \backslash B = \{1, 2, 3\}, \qquad B \backslash A = \{7, 8, 9\} \qquad \text{and so} \qquad A \oplus B = \{1, 2, 3, 7, 8, 9\}$$

Figure 1-7 is a Venn diagram in which $A \oplus B$ is shaded.

1.7 ALGEBRA OF SETS AND DUALITY

Sets under the operations of union, intersection, and complement satisfy various laws or identities which are listed in Table 1-1. In fact, we formally state this:

Theorem 1.3: Sets satisfy the laws in Table 1-1.

There are two methods of proving equations involving set operations. One way is to use what it means for an object x to be an element of each side, and the other way is to use Venn diagrams. For example, consider the first of DeMorgan's laws.

$$(A \cup B)^c = A^c \cap B^c$$

Table 1-1 Laws of the algebra of sets

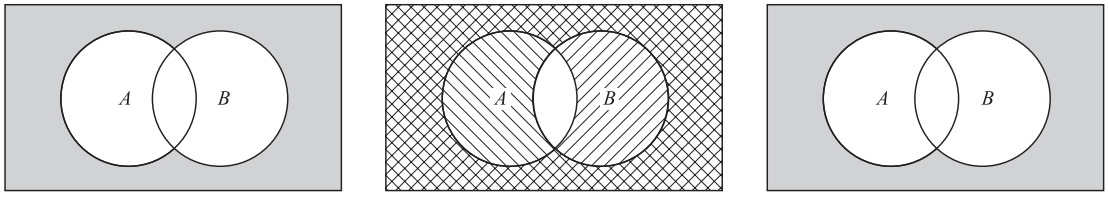
Idempotent laws	
(*1a*) $A \cup A = A$	(*1b*) $A \cap A = A$
Associative laws	
(*2a*) $(A \cup B) \cup C = A \cup (B \cup C)$	(*2b*) $(A \cap B) \cap C = A \cap (B \cap C)$
Commutative laws	
(*3a*) $A \cup B = B \cup A$	(*3b*) $A \cap B = B \cap A$
Distributive laws	
(*4a*) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	(*4b*) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
Identity laws	
(*5a*) $A \cup \varnothing = A$	(*5b*) $A \cap U = A$
(*6a*) $A \cup U = U$	(*6b*) $A \cap \varnothing = \varnothing$
Involution laws	
(*7*) $(A^c)^c = A$	
Complement laws	
(*8a*) $A \cup A^c = U$	(*8b*) $A \cap A^c = \varnothing$
(*9a*) $U^c = \varnothing$	(*9b*) $\varnothing^c = U$
DeMorgan's laws	
(*10a*) $(A \cup B)^c = A^c \cap B^c$	(*10b*) $(A \cap B)^c = A^c \cup B^c$

Method 1: We first show that $(A \cup B)^c \subseteq A^c \cap B^c$. If $x \in (A \cup B)^c$, then $x \notin A \cup B$. Thus $x \notin A$ and $x \notin B$, and so $x \in A^c$ and $x \in B^c$. Hence $x \in A^c \cap B^c$.

Next we show that $A^c \cap B^c \subseteq (A \cup B)^C$. Let $x \in A^c \cap B^c$. Then $x \in A^c$ and $x \in B^c$, so $x \notin A$ and $x \notin B$. Hence $x \notin A \cup B$, so $x \in (A \cup B)^c$.

We have proven that every element of $(A \cup B)^c$ belongs to $A^c \cap B^c$ and that every element of $A^c \cap B^c$ belongs to $(A \cup B)^c$. Together, these inclusions prove that the sets have the same elements, i.e., that $(A \cup B)^c = A^c \cap B^c$.

Method 2: From the Venn diagram for $A \cup B$ in Fig. 1-4, we see that $(A \cup B)^c$ is represented by the shaded area in Fig. 1-8(*a*). To find $A^c \cap B^c$, the area in both A^c and B^c, we shaded A^c with strokes in one direction and B^c with strokes in another direction as in Fig. 1-8(*b*). Then $A^c \cap B^c$ is represented by the crosshatched area, which is shaded in Fig. 1-8(*c*). Since $(A \cup B)^c$ and $A^c \cap B^c$ are represented by the same area, they are equal.



(*a*) $(A \cup B)^c$ is shaded (*b*) A^c is shaded with ////, B^c is shaded with \\\\ (*c*) $A^c \cap B^c$ is shaded

Fig. 1-8

Duality

Note that the identities in Table 1-1 are arranged in pairs, as, for example, (2*a*) and (2*b*). We now consider the principle behind this arrangement. Suppose E is an equation of set algebra. The *dual* E^* of E is the equation obtained by replacing each occurrence of $\cup$, $\cap$, U, and $\varnothing$ in E by $\cap$, $\cup$, $\varnothing$ and U, respectively. For example, the dual of

$$(U \cap A) \cup (B \cap A) = A \qquad \text{is} \qquad (\varnothing \cup A) \cap (B \cup A) = A$$

Observe that the pairs of laws in Table 1-1 are duals of each other. It is a fact of set algebra, called the *principle of duality*, that, if any equation E is an identity, then its dual E^* is also an identity.

1.8 FINITE SETS, COUNTING PRINCIPLE

A set is said to be finite if it contains exactly m distinct elements where m denotes some nonnegative integer. Otherwise, a set is said to be infinite. For example, the empty set $\varnothing$ and the set of letters of the English alphabet are finite sets, whereas the set of even positive integers, $\{2, 4, 6, \ldots\}$, is infinite.

The notation $n(A)$ will denote the number of elements in a finite set A. Some texts use $\#(A)$, $|A|$ or $\text{card}(A)$ instead of $n(A)$.

Lemma 1.4: If A and B are disjoint finite sets, then $A \cup B$ is finite and

$$n(A \cup B) = n(A) + n(B)$$

Proof. In counting the elements of $A \cup B$, first count those that are in A. There are $n(A)$ of these. The only other elements of $A \cup B$ are those that are in B but not in A. But since A and B are disjoint, no element of B is in A, so there are $n(B)$ elements that are in B but not in A. Therefore, $n(A \cup B) = n(A) + n(B)$.

We also have a formula for $n(A \cup B)$ even when they are not disjoint. This is proved in Problem 1.28.

Theorem 1.5: If A and B are finite sets, then $A \cup B$ and $A \cap B$ are finite and

$$n(A \cup B) = n(A) + n(B) - n(A \cap B)$$

We can apply this result to obtain a similar formula for three sets:

Corollary 1.6: If A, B, and C are finite sets, then so is $A \cup B \cup C$, and

$$n(A \cup B \cup C) = n(A) + n(B) + n(C) - n(A \cap B) - n(A \cap C) - n(B \cap C) + n(A \cap B \cap C)$$

Mathematical induction (Section 1.10) may be used to further generalize this result to any finite number of sets.

EXAMPLE 1.7 Consider the following data for 120 mathematics students at a college concerning the languages French, German, and Russian:

65 study French
45 study German
42 study Russian
20 study French and German
25 study French and Russian
15 study German and Russian
8 study all three languages.

Let F, G, and R denote the sets of students studying French, German and Russian, respectively. We wish to find the number of students who study at least one of the three languages, and to fill in the correct number of students in each of the eight regions of the Venn diagram shown in Fig. 1-9.

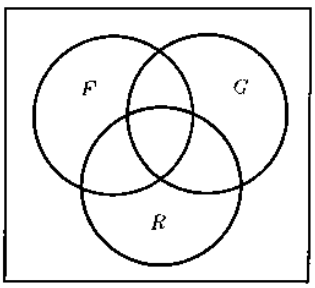


Fig. 1-9

By Corollary 1.6,

$$(F \cup G \cup R) = n(F) + n(G) + n(R) - n(F \cap G) - n(F \cap R) - n(G \cap R) + n(F \cap G \cap R)$$
$$= 65 + 45 + 42 - 20 - 25 - 15 + 8 = 100$$

That is, $n(F \cup G \cup R) = 100$ students study at least one of the three languages.

We now use this result to fill in the Venn diagram. We have:

8 study all three languages,

$20 - 8 = 12$ study French and German but not Russian

$25 - 8 = 17$ study French and Russian but not German

$15 - 8 = 7$ study German and Russian but not French

$65 - 12 - 8 - 17 = 28$ study only French

$45 - 12 - 8 - 7 = 18$ study only German

$42 - 17 - 8 - 7 = 10$ study only Russian

$120 - 100 = 20$ do not study any of the languages

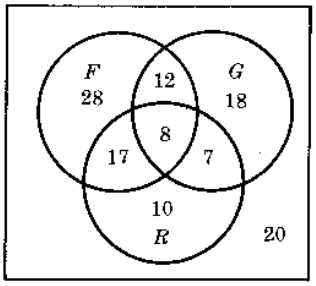


Fig. 1-10

Accordingly, the completed diagram appears in Fig. 1-10. Observe that $28 + 18 + 10 = 56$ students study only one of the languages.

1.9 CLASSES OF SETS, POWER SETS, PARTITIONS

Given a set S, we might wish to talk about some of its subsets. Thus we would be considering a set of sets. Whenever such a situation occurs, to avoid confusion we will speak of a *class* of sets or *collection* of sets rather than a set of sets. If we wish to consider some of the sets in a given class of sets, then we speak of a *subclass* or *subcollection*.

EXAMPLE 1.8 Suppose $S = \{1, 2, 3, 4\}$. Let $\mathcal{A}$ be the class of subsets of S which contain exactly three elements of S. Then

$$\mathcal{A} = [\{1, 2, 3\}, \{1, 2, 4\}, \{1, 3, 4\}, \{2, 3, 4\}]$$

The elements of $\mathcal{A}$ are the sets $\{1, 2, 3\}$, $\{1, 2, 4\}$, $\{1, 3, 4\}$, and $\{2, 3, 4\}$.

Let $\mathcal{B}$ be the class of subsets of S which contain 2 and two other elements of S. Then

$$\mathcal{B} = [\{1, 2, 3\}, \{1, 2, 4\}, \{2, 3, 4\}]$$

The elements of $\mathcal{B}$ are the sets $\{1, 2, 3\}$, $\{1, 2, 4\}$, and $\{2, 3, 4\}$. Thus $\mathcal{B}$ is a subclass of $\mathcal{A}$, since every element of $\mathcal{B}$ is also an element of $\mathcal{A}$. (To avoid confusion, we will sometimes enclose the sets of a class in brackets instead of braces.)

Power Sets

For a given set S, we may speak of the class of all subsets of S. This class is called the *power set* of S, and will be denoted by Power(S). If S is finite, then so is Power(S). In fact, the number of elements in Power(S) is 2 raised to the power of S; that is,

$$n(\text{Power}(S)) = 2^{n(S)}$$

(For this reason, the power set of S is sometimes denoted by 2^S.)

EXAMPLE 1.9 Suppose $S = \{1, 2, 3\}$. Then

$$\text{Power}(S) = [\varnothing, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, S]$$

Note that the empty set $\varnothing$ belongs to Power(S) since $\varnothing$ is a subset of S. Similarly, S belongs to Power(S). As expected from the above remark, Power(S) has $2^3 = 8$ elements.

Partitions

Let S be a nonempty set. A partition of S is a subdivision of S into nonoverlapping, nonempty subsets. Precisely, a *partition* of S is a collection $\{A_i\}$ of nonempty subsets of S such that:

(i) Each a in S belongs to one of the A_i.

(ii) The sets of $\{A_i\}$ are mutually disjoint; that is, if
$$A_i \neq A_j \qquad \text{then} \qquad A_i \cap A_j = \varnothing$$

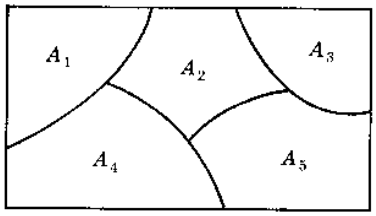


Fig. 1-11

The subsets in a partition are called *cells*. Figure 1-11 is a Venn diagram of a partition of the rectangular set S of points into five cells, A_1, A_2, A_3, A_4, and A_5.

EXAMPLE 1.10 Consider the following collections of subsets of $S = \{1, 2, \ldots, 8, 9\}$:

(i) $[\{1,3,5\}, \{2,6\}, \{4,8,9\}]$

(ii) $[\{1,3,5\}, \{2,4,6,8\}, \{5,7,9\}]$

(iii) $[\{1,3,5\}, \{2,4,6,8\}, \{7,9\}]$

Then (i) is not a partition of S since 7 in S does not belong to any of the subsets. Furthermore, (ii) is not a partition of S since $\{1,3,5\}$ and $\{5,7,9\}$ are not disjoint. On the other hand, (iii) is a partition of S.

Generalized Set Operations

The set operations of union and intersection were defined above for two sets. These operations can be extended to any number of sets, finite or infinite, as follows.

Consider first a finite number of sets, say, $A_1, A_2, \ldots, A_m$. The union and intersection of these sets are denoted and defined, respectively, by

$$A_1 \cup A_2 \cup \cdots \cup A_m = \cup_{i=1}^{m} A_i = \{x: x \in A_i \text{ for some } A_i\}$$
$$A_1 \cap A_2 \cap \cdots \cap A_m = \cap_{i=1}^{m} A_i = \{x: x \in A_i \text{ for every } A_i\}$$

That is, the union consists of those elements which belong to at least one of the sets, and the intersection consists of those elements which belong to all the sets.

Now let $\mathcal{A}$ be any collection of sets. The union and the intersection of the sets in the collection $\mathcal{A}$ is denoted and defined, respectively, by

$$\cup(A: A \in \mathcal{A}) = \{x: x \in A \text{ for some } A \in \mathcal{A}\}$$
$$\cap(A: A \in \mathcal{A}) = \{x: x \in A \text{ for every } A \in \mathcal{A}\}$$

That is, the union consists of those elements which belong to at least one of the sets in the collection $\mathcal{A}$, and the intersection consists of those elements which belong to every set in the collection $\mathcal{A}$.

EXAMPLE 1.11 Consider the sets

$$A_1 = \{1,2,3,\ldots\} = \mathbf{N}, \qquad A_2 = \{2,3,4,\ldots\}, \qquad A_3 = \{3,4,5,\ldots\}, \qquad A_n = \{n, n+1, n+2, \ldots\}$$

Then the union and intersection of the sets are as follows:

$$\cup(A_n: n \in \mathbf{N}) = \mathbf{N} \qquad \text{and} \qquad \cap(A_n: n \in \mathbf{N}) = \varnothing$$

DeMorgan's laws also hold for the above generalized operations. That is:

Theorem 1.7: Let $\mathcal{A}$ be a collection of sets. Then

(i) $(\cup(A: A \in \mathcal{A}))^c = \cap(A^c: A \in \mathcal{A})$

(ii) $(\cap(A: A \in \mathcal{A}))^c = \cup(A^c: A \in \mathcal{A})$

1.10 MATHEMATICAL INDUCTION

An essential property of the set

$$\mathbf{N} = \{1, 2, 3, \ldots\}$$

which is used in many proofs, follows:

Principle of Mathematical Induction I: Let P be a proposition defined on the positive integers $\mathbf{N}$, i.e., $P(n)$ is either true or false for each n in $\mathbf{N}$. Suppose P has the following two properties:

(i) $P(1)$ is true.

(ii) $P(n+1)$ is true whenever $P(n)$ is true.

Then P is true for every positive integer.

We shall not prove this principle. In fact, this principle is usually given as one of the axioms when $\mathbf{N}$ is developed axiomatically.

EXAMPLE 1.12 Let P be the proposition that the sum of the first n odd numbers is n^2; that is,

$$P(n)\colon\ 1 + 3 + 5 + \ldots + (2n-1) = n^2$$

(The nth odd number is $2n-1$, and the next odd number is $2n+1$). Observe that $P(n)$ is true for $n = 1$, that is,

$$P(1)\colon\ 1 = 1^2$$

Assuming $P(n)$ is true, we add $2n+1$ to both sides of $P(n)$, obtaining

$$1 + 3 + 5 + \ldots + (2n-1) + (2n+1) = n^2 + (2n+1) = (n+1)^2$$

which is $P(n+1)$. That is, $P(n+1)$ is true whenever $P(n)$ is true. By the principle of mathematical induction, P is true for all n.

There is a form of the principle of mathematical induction which is sometimes more convenient to use. Although it appears different, it is really equivalent to the principle of induction.

Principle of Mathematical Induction II: Let P be a proposition defined on the positive integers $\mathbf{N}$ such that:

(i) $P(1)$ is true.

(ii) $P(n)$ is true whenever $P(k)$ is true for all $1 \leq k < n$.

Then P is true for every positive integer.

Remark: Sometimes one wants to prove that a proposition P is true for the set of integers

$$\{a,\ a+1,\ a+2, \ldots\}$$

where a is any integer, possibly zero. This can be done by simply replacing 1 by a in either of the above Principles of Mathematical Induction.

Solved Problems

SETS AND SUBSETS

1.1. Which of these sets are equal: $\{r, t, s\}$, $\{s, t, r, s\}$, $\{t, s, t, r\}$, $\{s, r, s, t\}$?

They are all equal. Order and repetition do not change a set.

1.2. List the elements of the following sets; here $\mathbf{N} = \{1, 2, 3, \ldots\}$.

(*a*) $A = \{x: x \in \mathbf{N},\ 3 < x < 12\}$

(*b*) $B = \{x: x \in \mathbf{N},\ x \text{ is even},\ x < 15\}$

(*c*) $C = \{x: x \in \mathbf{N},\ 4 + x = 3\}$.

(*a*) A consists of the positive integers between 3 and 12; hence

$$A = \{4, 5, 6, 7, 8, 9, 10, 11\}$$

(*b*) B consists of the even positive integers less than 15; hence

$$B = \{2, 4, 6, 8, 10, 12, 14\}$$

(*c*) There are no positive integers which satisfy the condition $4 + x = 3$; hence C contains no elements. In other words, $C = \varnothing$, the empty set.

1.3. Consider the following sets:

$$\varnothing, \quad A = \{1\}, \quad B = \{1, 3\}, \quad C = \{1, 5, 9\}, \quad D = \{1, 2, 3, 4, 5\},$$
$$E = \{1, 3, 5, 7, 9\}, \quad U = \{1, 2, \ldots, 8, 9\}$$

Insert the correct symbol $\subseteq$ or $\nsubseteq$ or between each pair of sets:

(*a*) $\varnothing$, A (*c*) B, C (*e*) C, D (*g*) D, E

(*b*) A, B (*d*) B, E (*f*) C, E (*h*) D, U

(*a*) $\varnothing \subseteq A$ because $\varnothing$ is a subset of every set.

(*b*) $A \subseteq B$ because 1 is the only element of A and it belongs to B.

(*c*) $B \nsubseteq C$ because $3 \in B$ but $3 \notin C$.

(*d*) $B \nsubseteq E$ because the elements of B also belong to E.

(*e*) $C \nsubseteq D$ because $9 \in C$ but $9 \notin D$.

(*f*) $C \subseteq E$ because the elements of C also belong to E.

(*g*) $D \nsubseteq E$ because $2 \in D$ but $2 \notin E$.

(*h*) $D \subseteq U$ because the elements of D also belong to U.

1.4. Show that $A = \{2, 3, 4, 5\}$ is not a subset of $B = \{x: x \in \mathbf{N},\ x \text{ is even}\}$.

It is necessary to show that at least one element in A does not belong to B. Now $3 \in A$ and, since B consists of even numbers, $3 \notin B$; hence A is not a subset of B.

1.5. Show that $A = \{2, 3, 4, 5\}$ is a proper subset of $C = \{1, 2, 3, \ldots, 8, 9\}$.

Each element of A belongs to C so $A \subseteq C$. On the other hand, $1 \in C$ but $1 \notin A$. Hence $A \neq C$. Therefore A is a proper subset of C.

SET OPERATIONS

Problems 1.6 to 1.8 refer to the universal set $U = \{1, 2, \ldots, 9\}$ and the sets

$$A = \{1, 2, 3, 4, 5\}, \quad C = \{5, 6, 7, 8, 9\}, \quad E = \{2, 4, 6, 8\}$$
$$B = \{4, 5, 6, 7\}, \quad D = \{1, 3, 5, 7, 9\}, \quad F = \{1, 5, 9\}$$

1.6. Find:

(*a*) $A \cup B$ and $A \cap B$ (*c*) $A \cup C$ and $A \cap C$ (*e*) $E \cup E$ and $E \cap E$
(*b*) $B \cup D$ and $B \cap D$ (*d*) $D \cup E$ and $D \cap E$ (*f*) $D \cup F$ and $D \cap F$

Recall that the union $X \cup Y$ consists of those elements in either X or Y (or both), and that the intersection $X \cap Y$ consists of those elements in both X and Y.

(*a*) $A \cup B = \{1,2,3,4,5,6,7\}$ $A \cap B = \{4,5\}$
(*b*) $B \cup D = \{1,3,4,5,6,7,9\}$ $B \cap D = \{5,7\}$
(*c*) $A \cup C = \{1,2,3,4,5,6,7,8,9\} = U$ $A \cap C = \{5\}$
(*d*) $D \cap E = \{1,2,3,4,5,6,7,8,9\} = U$ $D \cap E = \varnothing$
(*e*) $E \cup E = \{2,4,6,8\} = E$ $E \cap E = \{2,4,6,8\} = E$
(*f*) $D \cup F = \{1,3,5,7,9\} = D$ $D \cap F = \{1,5,9\} = F$

Observe that $F \subseteq D$; so by Theorem 1.2 we must have $D \cup F = D$ and $D \cap F = F$.

1.7. Find: (*a*) A^c, B^c, D^c, E^c; (*b*) $A\backslash B$, $B\backslash A$, $D\backslash E$, $F\backslash D$; (*c*) $A \oplus B$, $C \oplus D$, $E \oplus F$.

Recall that:

(1) The complement X^c consists of those elements in the universal set U which do not belong to X.
(2) The difference $X\backslash Y$ consist of the elements in X which do not belong to Y.
(3) The symmetric difference $X \oplus Y$ consists of the elements in X or in Y but not in both X and Y.

Therefore:

(*a*) $A^c = \{6,7,8,9\}$; $B^c = \{1,2,3,8,9\}$; $D^c = \{2,4,6,8\} = E$; $E^c = \{1,3,5,7,9\} = D$.
(*b*) $A\backslash B = \{1,2,3\}$; $B\backslash A = \{6,7\}$; $D\backslash E = \{1,3,5,7,9\} = D$; $F\backslash D = \varnothing$.
(*c*) $A \oplus B = \{1,2,3,6,7\}$; $C \oplus D = \{1,3,8,9\}$; $E \oplus F = \{2,4,6,8,1,5,9\} = E \cup F$.

1.8. Find: (*a*) $A \cap (B \cup E)$; (*b*) $(A\backslash E)^c$;
(*c*) $(A \cap D)\backslash B$; (*d*) $(B \cap F) \cup (C \cap E)$.

(*a*) First compute $B \cup E = \{2,4,5,6,7,8\}$. Then $A \cap (B \cup E) = \{2,4,5\}$.
(*b*) $A\backslash E = \{1,3,5\}$. Then $(A\backslash E)^c = \{2,4,6,7,8,9\}$.
(*c*) $A \cap D = \{1,3,5\}$. Now $(A \cap D)\backslash B = \{1,3\}$.
(*d*) $B \cap F = \{5\}$ and $C \cap E = \{6,8\}$. So $(B \cap F) \cup (C \cap E) = \{5,6,8\}$.

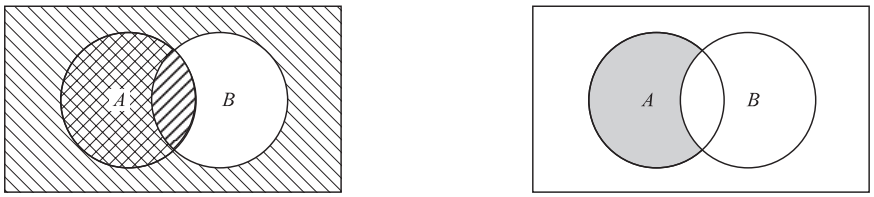
1.9. Show that we can have $A \cap B = A \cap C$ without $B = C$.

Let $A = \{1,2\}$, $B = \{2,3\}$, and $C = \{2,4\}$. Then $A \cap B = \{2\}$ and $A \cap C = \{2\}$. Thus $A \cap B = A \cap C$ but $B \neq C$.

VENN DIAGRAMS

1.10. Consider the Venn diagram of two arbitrary sets A and B in Fig. 1-1(*c*). Shade the sets: (*a*) $A \cap B^c$; (*b*) $(B\backslash A)^c$.

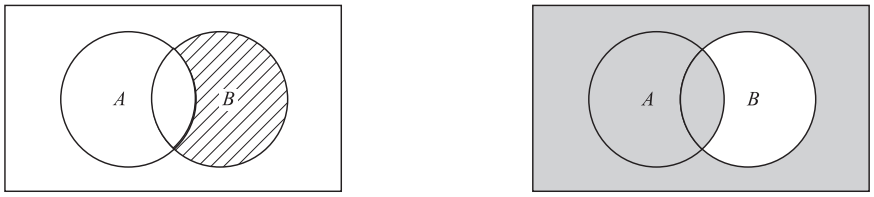
(*a*) First shade the area represented by A with strokes in one direction (///), and then shade the area represented by B^c (the area outside B), with strokes in another direction (\\\). This is shown in Fig. 1-12(*a*). The cross-hatched area is the intersection of these two sets and represents $A \cap B^c$ and this is shown in Fig. 1-12(*b*). Observe that $A \cap B^c = A\backslash B$. In fact, $A\backslash B$ is sometimes defined to be $A \cap B^c$.



(*a*) A and B^c are shaded (*b*) $A \cap B^c$ is shaded

Fig. 1-12

(*b*) First shade the area represented by $B \backslash A$ (the area of B which does not lie in A) as in Fig. 1-13(*a*). Then the area outside this shaded region, which is shown in Fig. 1-13(*b*), represents $(B \backslash A)^c$.



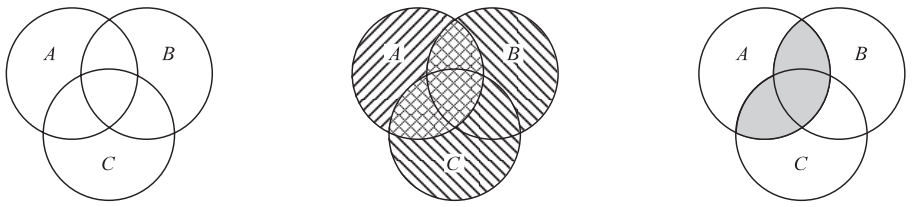
(*a*) $B \setminus A$ is shaded (*b*) $(B \setminus A)^c$ is shaded

Fig. 1-13

1.11. Illustrate the distributive law $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ with Venn diagrams.

Draw three intersecting circles labeled A, B, C, as in Fig. 1-14(*a*). Now, as in Fig. 1-14(*b*) shade A with strokes in one direction and shade $B \cup C$ with strokes in another direction; the crosshatched area is $A \cap (B \cup C)$, as in Fig. 1-14(*c*). Next shade $A \cap B$ and then $A \cap C$, as in Fig. 1-14(*d*); the total area shaded is $(A \cap B) \cup (A \cap C)$, as in Fig. 1-14(*e*).

As expected by the distributive law, $A \cap (B \cup C)$ and $(A \cap B) \cup (A \cap C)$ are both represented by the same set of points.



(*a*) (*b*) A and $B \cup C$ are shaded (*c*) $A \cap (B \cup C)$ is shaded

(*d*) $A \cap B$ and A $\cap$ C are shaded (*e*) $(A \cap B) \cup$ (A $\cap$ C) is shaded

Fig. 1-14

1.12. Determine the validity of the following argument:

S_1: All my friends are musicians.
S_2: John is my friend.
S_3: None of my neighbors are musicians.

S: John is not my neighbor.

The premises S_1 and S_3 lead to the Venn diagram in Fig. 1-15. By S_2, John belongs to the set of friends which is disjoint from the set of neighbors. Thus S is a valid conclusion and so the argument is valid.

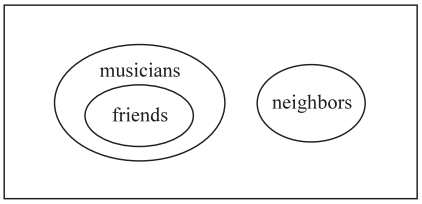


Fig. 1-15

FINITE SETS AND THE COUNTING PRINCIPLE

1.13. Determine which of the following sets are finite.

(*a*) $A = \{\text{seasons in the year}\}$
(*b*) $B = \{\text{states in the Union}\}$
(*c*) $C = \{\text{positive integers less than 1}\}$
(*d*) $D = \{\text{odd integers}\}$
(*e*) $E = \{\text{positive integral divisors of 12}\}$
(*f*) $F = \{\text{cats living in the United States}\}$

(*a*) A is finite since there are four seasons in the year, i.e., $n(A) = 4$.
(*b*) B is finite because there are 50 states in the Union, i.e. $n(B) = 50$.
(*c*) There are no positive integers less than 1; hence C is empty. Thus C is finite and $n(C) = 0$.
(*d*) D is infinite.
(*e*) The positive integer divisors of 12 are 1, 2, 3, 4, 6, and 12. Hence E is finite and $n(E) = 6$.
(*f*) Although it may be difficult to find the number of cats living in the United States, there is still a finite number of them at any point in time. Hence F is finite.

1.14. In a survey of 60 people, it was found that:

25 read *Newsweek* magazine
26 read *Time*
26 read *Fortune*
9 read both *Newsweek* and *Fortune*
11 read both *Newsweek* and *Time*
8 read both *Time* and *Fortune*
3 read all three magazines

(*a*) Find the number of people who read at least one of the three magazines.
(*b*) Fill in the correct number of people in each of the eight regions of the Venn diagram in Fig. 1-16(*a*) where N, T, and F denote the set of people who read *Newsweek*, *Time*, and *Fortune*, respectively.

(*c*) Find the number of people who read exactly one magazine.

(*a*) We want $n(N \cup T \cup F)$. By Corollary 1.6,

$$n(N \cup T \cup F) = n(N) + n(T) + n(F) - n(N \cap T) - n(N \cap F) - n(T \cap F) + n(N \cap T \cap F)$$
$$= 25 + 26 + 26 - 11 - 9 - 8 + 3 = 52.$$

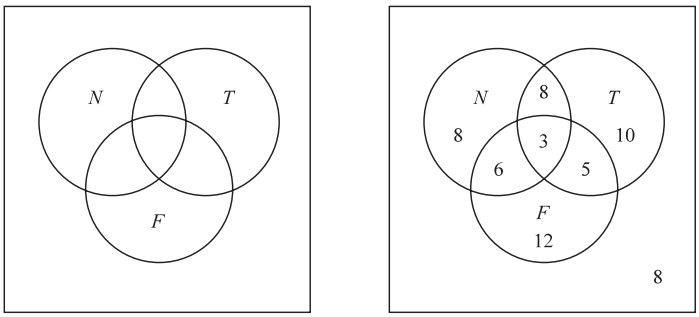


Fig. 1-16

(*b*) The required Venn diagram in Fig. 1-16(*b*) is obtained as follows:

3 read all three magazines
$11 - 3 = 8$ read *Newsweek* and *Time* but not all three magazines
$9 - 3 = 6$ read *Newsweek* and *Fortune* but not all three magazines
$8 - 3 = 5$ read *Time* and *Fortune* but not all three magazines
$25 - 8 - 6 - 3 = 8$ read only *Newsweek*
$26 - 8 - 5 - 3 = 10$ read only *Time*
$26 - 6 - 5 - 3 = 12$ read only *Fortune*
$60 - 52 = 8$ read no magazine at all

(*c*) $8 + 10 + 12 = 30$ read only one magazine.

ALGEBRA OF SETS AND DUALITY

1.15. Write the dual of each set equation:

(*a*) $(U \cap A) \cup (B \cap A) = A$
(*b*) $(A \cup B \cup C)^c = (A \cup C)^c \cap (A \cup B)^c$
(*c*) $(A \cap U) \cap (\varnothing \cup A^c) = \varnothing$
(*d*) $(A \cap U)^c \cap A = \varnothing$

Interchange $\cup$ and $\cap$ and also U and $\varnothing$ in each set equation:

(*a*) $(\varnothing \cup A) \cap (B \cup A) = A$
(*b*) $(A \cap B \cap C)^c = (A \cap C)^c \cup (A \cap B)^c$
(*c*) $(A \cup \varnothing) \cup (U \cap A^c) = U$
(*d*) $(A \cup \varnothing)^c \cup A = U$

1.16. Prove the Commutative laws: (*a*) $A \cup B = B \cup A$, and (*b*) $A \cap B = B \cap A$.

(*a*) $A \cup B = \{x: x \in A \text{ or } x \in B\} = \{x: x \in B \text{ or } x \in A\} = B \cup A$.
(*b*) $A \cap B = \{x: x \in A \text{ and } x \in B\} = \{x: x \in B \text{ and } x \in A\} = B \cap A$.

1.17. Prove the following identity: $(A \cup B) \cap (A \cup B^c) = A$.

	Statement	Reason
1.	$(A \cup B) \cap (A \cup B^c) = A \cup (B \cap B^c)$	Distributive law
2.	$B \cap B^c = \varnothing$	Complement law
3.	$(A \cup B) \cap (A \cup B^c) = A \cup \varnothing$	Substitution
4.	$A \cup \varnothing = A$	Identity law
5.	$(A \cup B) \cap (A \cup B^c) = A$	Substitution

1.18. Prove $(A \cup B) \backslash (A \cap B) = (A \backslash B) \cup (B \backslash A)$. (Thus either one may be used to define $A \oplus B$.)

Using $X \backslash Y = X \cap Y^c$ and the laws in Table 1-1, including DeMorgan's laws, we obtain:

$$\begin{aligned}(A \cup B) \backslash (A \cap B) &= (A \cup B) \cap (A \cap B)^c = (A \cup B) \cap (A^c \cup B^c) \\ &= (A \cap A^c) \cup (A \cap B^c) \cup (B \cap A^c) \cup (B \cap B^c) \\ &= \varnothing \cup (A \cap B^c) \cup (B \cap A^c) \cup \varnothing \\ &= (A \cap B^c) \cup (B \cap A^c) = (A \backslash B) \cup (B \backslash A).\end{aligned}$$

CLASSES OF SETS

1.19. Find the elements of the set $A = [\{1, 2, 3\}, \{4, 5\}, \{6, 7, 8\}]$.

A is a class of sets; its elements are the sets $\{1, 2, 3\}$, $\{4, 5\}$, and $\{6, 7, 8\}$.

1.20. Consider the class A of sets in Problem 1.19. Determine whether each of the following is true or false:

(*a*) $1 \in A$ (*c*) $\{6, 7, 8\} \in A$ (*e*) $\varnothing \in A$

(*b*) $\{1, 2, 3\} \subseteq A$ (*d*) $\{\{4, 5\}\} \subseteq A$ (*f*) $\varnothing \subseteq A$

(*a*) False. 1 is not one of the elements of A.

(*b*) False. $\{1, 2, 3\}$ is not a subset of A; it is one of the elements of A.

(*c*) True. $\{6, 7, 8\}$ is one of the elements of A.

(*d*) True. $\{\{4, 5\}\}$, the set consisting of the element $\{4, 5\}$, is a subset of A.

(*e*) False. The empty set is not an element of A, i.e., it is not one of the three sets listed as elements of A.

(*f*) True. The empty set is a subset of every set; even a class of sets.

1.21. Determine the power set $\text{Power}(A)$ of $A = \{a, b, c, d\}$.

The elements of $\text{Power}(A)$ are the subsets of A. Hence

$$\begin{aligned}\text{Power}(A) = [&A, \{a, b, c\}, \{a, b, d\}, \{a, c, d\}, \{b, c, d\}, \{a, b\}, \{a, c\}, \\ &\{a, d\}, \{b, c\}, \{b, d\}, \{c, d\}, \{a\}, \{b\}, \{c\}, \{d\}, \varnothing]\end{aligned}$$

As expected, $\text{Power}(A)$ has $2^4 = 16$ elements.

1.22. Let $S = \{red, blue, green, yellow\}$. Determine which of the following is a partition of S:

(*a*) $P_1 = [\{red\}, \{blue, green\}]$. (*c*) $P_3 = [\varnothing, \{red, blue\}, \{green, yellow\}]$.

(*b*) $P_2 = [\{red, blue, green, yellow\}]$. (*d*) $P_4 = [\{blue\}\{red, yellow, green\}$.

(*a*) No, since *yellow* does not belong to any cell.

(*b*) Yes, since P_2 is a partition of S whose only element is S itself.

(*c*) No, since the empty set $\varnothing$ cannot belong to a partition.

(*d*) Yes, since each element of S appears in exactly one cell.

1.23. Find all partitions of $S = \{1, 2, 3\}$.

Note that each partition of S contains either 1, 2, or 3 cells. The partitions for each number of cells are as follows:

(1) : [S]

(2) : [{1}, {2, 3}], [{2}, {1, 3}], [{3}, {1, 2}]

(3) : [{1}, {2}, {3}]

Thus we see that there are five different partitions of S.

MISCELLANEOUS PROBLEMS

1.24. Prove the proposition P that the sum of the first n positive integers is $\frac{1}{2}n(n+1)$; that is,

$$P(n): \qquad 1 + 2 + 3 + \ldots + n = \frac{1}{2}n(n+1)$$

The proposition holds for $n = 1$ since

$$P(1) : 1 = \tfrac{1}{2}(1)(1+1)$$

Assuming $P(n)$ is true, we add $n+1$ to both sides of $P(n)$, obtaining

$$\begin{aligned} 1 + 2 + 3 + \ldots + n + (n+1) &= \tfrac{1}{2}n(n+1) + (n+1) \\ &= \tfrac{1}{2}[n(n+1) + 2(n+1)] \\ &= \tfrac{1}{2}[(n+1)(n+2)] \end{aligned}$$

which is $P(n+1)$. That is, $P(n+1)$ is true whenever $P(n)$ is true. By the principle of induction, P is true for all n.

1.25. Prove the following proposition (for $n \geq 0$):

$$P(n): \quad 1 + 2 + 2^2 + 2^3 + \cdots + 2^n = 2^{n+1} - 1$$

$P(0)$ is true since $1 = 2^1 - 1$. Assuming $P(n)$ is true, we add 2^{n+1} to both sides of $P(n)$, obtaining

$$\begin{aligned} 1 + 2^1 + 2^2 + \cdots + 2^n + 2^{n+1} &= 2^{n+1} - 1 + 2^{n+1} \\ &= 2(2^{n+1}) - 1 \\ &= 2^{n+2} - 1 \end{aligned}$$

which is $P(n+1)$. Thus $P(n+1)$ is true whenever $P(n)$ is true. By the principle of induction, P is true for all $n \geq 0$.

1.26. Prove: $(A \cap B) \subseteq A \subseteq (A \cup B)$ and $(A \cap B) \subseteq B \subseteq (A \cup B)$.

Since every element in $A \cap B$ is in both A and B, it is certainly true that if $x \in (A \cap B)$ then $x \in A$; hence $(A \cap B) \subseteq A$. Furthermore, if $x \in A$, then $x \in (A \cup B)$ (by the definition of $A \cup B$), so $A \subseteq (A \cup B)$. Putting these together gives $(A \cap B) \subseteq A \subseteq (A \cup B)$. Similarly, $(A \cap B) \subseteq B \subseteq (A \cup B)$.

1.27. Prove Theorem 1.2: The following are equivalent: $A \subseteq B$, $A \cap B = A$, and $A \cup B = B$.

Suppose $A \subseteq B$ and let $x \in A$. Then $x \in B$, hence $x \in A \cap B$ and $A \subseteq A \cap B$. By Problem 1.26, $(A \cap B) \subseteq A$. Therefore $A \cap B = A$. On the other hand, suppose $A \cap B = A$ and let $x \in A$. Then $x \in (A \cap B)$, hence $x \in A$ and $x \in B$. Therefore, $A \subseteq B$. Both results show that $A \subseteq B$ is equivalent to $A \cap B = A$.

Suppose again that $A \subseteq B$. Let $x \in (A \cup B)$. Then $x \in A$ or $x \in B$. If $x \in A$, then $x \in B$ because $A \subseteq B$. In either case, $x \in B$. Therefore $A \cup B \subseteq B$. By Problem 1.26, $B \subseteq A \cup B$. Therefore $A \cup B = B$. Now suppose $A \cup B = B$ and let $x \in A$. Then $x \in A \cup B$ by definition of union sets. Hence $x \in B = A \cup B$. Therefore $A \subseteq B$. Both results show that $A \subseteq B$ is equivalent to $A \cup B = B$.

Thus $A \subseteq B$, $A \cap B = A$ and $A \cup B = B$ are equivalent.

1.28. Prove Theorem 1.5: If A and B are finite sets, then $A \cup B$ and $A \cap B$ are finite and

$$n(A \cup B) = n(A) + n(B) - n(A \cap B)$$

If A and B are finite, then clearly $A \cap B$ and $A \cup B$ are finite.

Suppose we count the elements of A and then count the elements of B. Then every element in $A \cap B$ would be counted twice, once in A and once in B. Hence

$$n(A \cup B) = n(A) + n(B) - n(A \cap B)$$

Alternatively, (Problem 1.36) A is the disjoint union of $A \backslash B$ and $A \cap B$, B is the disjoint union of $B \backslash A$ and $A \cap B$, and $A \cup B$ is the disjoint union of $A \backslash B$, $A \cap B$, and $B \backslash A$. Therefore, by Lemma 1.4,

$$\begin{aligned} n(A \cup B) &= n(A \backslash B) + n(A \cap B) + n(B \backslash A) \\ &= n(A \backslash B) + n(A \cap B) + n(B \backslash A) + n(A \cap B) - n(A \cap B) \\ &= n(A) + n(B) - n(A \cap B) \end{aligned}$$

Supplementary Problems

SETS AND SUBSETS

1.29. Which of the following sets are equal?

$A = \{x\colon x^2 - 4x + 3 = 0\}$, $C = \{x\colon x \in \mathbf{N}, x < 3\}$, $E = \{1, 2\}$, $G = \{3, 1\}$

$B = \{x\colon x^2 - 3x + 2 = 0\}$, $D = \{x\colon x \in \mathbf{N}, x \text{ is odd}, x < 5\}$, $F = \{1, 2, 1\}$, $H = \{1, 1, 3\}$

1.30. List the elements of the following sets if the universal set is $U = \{a, b, c, \ldots, y, z\}$. Furthermore, identify which of the sets, if any, are equal.

$A = \{x\colon x \text{ is a vowel}\}$ $C = \{x\colon x \text{ precedes f in the alphabet}\}$

$B = \{x\colon x \text{ is a letter in the word ``}\textit{little}\text{''}\}$ $D = \{x\colon x \text{ is a letter in the word ``}\textit{title}\text{''}\}$

1.31. Let $A = \{1, 2, \ldots, 8, 9\}$, $B = \{2, 4, 6, 8\}$, $C = \{1, 3, 5, 7, 9\}$, $D = \{3, 4, 5\}$, $E = \{3, 5\}$.

Which of the above sets can equal a set X under each of the following conditions?

(*a*) X and B are disjoint. (*c*) $X \subseteq A$ but $X \nsubseteq C$.

(*b*) $X \subseteq D$ but $X \nsubseteq B$. (*d*) $X \subseteq C$ but $X \nsubseteq A$.

SET OPERATIONS

Problems 1.32 to 1.34 refer to the sets $U = \{1, 2, 3, \ldots, 8, 9\}$ and $A = \{1, 2, 5, 6\}$, $B = \{2, 5, 7\}$, $C = \{1, 3, 5, 7, 9\}$.

1.32. Find: (*a*) $A \cap B$ and $A \cap C$; (*b*) $A \cup B$ and $B \cup C$; (*c*) A^c and C^c.

1.33. Find: (*a*) $A\backslash B$ and $A\backslash C$; (*b*) $A \oplus B$ and $A \oplus C$.

1.34. Find: (*a*) $(A \cup C)\backslash B$; (*b*) $(A \cup B)^c$; (*c*) $(B \oplus C)\backslash A$.

1.35. Let $A = \{a, b, c, d, e\}$, $B = \{a, b, d, f, g\}$, $C = \{b, c, e, g, h\}$, $D = \{d, e, f, g, h\}$.

Find:

(*a*)	$A \cup B$	(*d*)	$A \cap (B \cup D)$	(*g*)	$(A \cup D)\backslash C$	(*j*)	$A \oplus B$
(*b*)	$B \cap C$	(*e*)	$B\backslash(C \cup D)$	(*h*)	$B \cap C \cap D$	(*k*)	$A \oplus C$
(*c*)	$C\backslash D$	(*f*)	$(A \cap D) \cup B$	(*i*)	$(C\backslash A)\backslash D$	(*l*)	$(A \oplus D)\backslash B$

1.36. Let A and B be any sets. Prove:

(*a*) A is the disjoint union of $A\backslash B$ and $A \cap B$.

(*b*) $A \cup B$ is the disjoint union of $A\backslash B$, $A \cap B$, and $B\backslash A$.

1.37. Prove the following:

(*a*) $A \subseteq B$ if and only if $A \cap B^c = \varnothing$.

(*b*) $A \subseteq B$ if and only if $A^c \cup B = U$.

(*c*) $A \subseteq B$ if and only if $B^c \subseteq A^c$.

(*d*) $A \subseteq B$ if and only if $A\backslash B = \varnothing$.

(Compare results with Theorem 1.2.)

1.38. Prove the Absorption laws: (*a*) $A \cup (A \cap B) = A$; (*b*) $A \cap (A \cup B) = A$.

1.39. The formula $A\backslash B = A \cap B^c$ defines the difference operation in terms of the operations of intersection and complement. Find a formula that defines the union $A \cup B$ in terms of the operations of intersection and complement.

VENN DIAGRAMS

1.40. The Venn diagram in Fig. 1-17 shows sets A, B, C. Shade the following sets: (*a*) $A\backslash(B \cup C)$; (*b*) $A^c \cap (B \cup C)$; (*c*) $A^c \cap (C\backslash B)$.

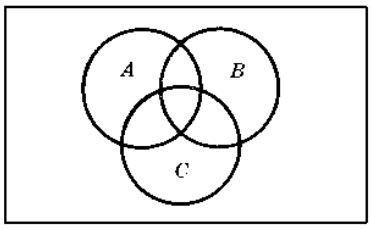


Fig. 1-17

1.41. Use the Venn diagram Fig. 1-6 and Example 1.6 to write each set as the (disjoint) union of fundamental products:

(*a*) $A \cap (B \cup C)$, (*b*) $A^c \cap (B \cup C)$, (*c*) $A \cup (B \backslash C)$.

1.42. Draw a Venn diagram of sets A, B, C where $A \subseteq B$, sets B and C are disjoint, but A and C have elements in common.

ALGEBRA OF SETS AND DUALITY

1.43. Write the dual of each equation:

(*a*) $A \cup B = (B^c \cap A^c)^c$ (*b*) $A = (B^c \cap A) \cup (A \cap B)$

(*c*) $A \cup (A \cap B) = A$ (*d*) $(A \cap B) \cup (A^c \cap B) \cup (A \cap B^c) \cup (A^c \cap B^c) = U$

1.44. Use the laws in Table 1-1 to prove each set identity:

(*a*) $(A \cap B) \cup (A \cap B^c) = A$.

(*b*) $A \cup (A \cap B) = A$.

(*c*) $A \cup B = (A \cap B^c) \cup (A^c \cap B) \cup (A \cap B)$.

FINITE SETS AND THE COUNTING PRINCIPLE

1.45. Determine which of the following sets are finite:

(*a*) The set of lines parallel to the x axis

(*b*) The set of letters in the English alphabet

(*c*) The set of numbers which are multiples of 5

(*d*) The set of animals living on the earth

(*e*) The set of numbers which are solutions of the equation:

$$x^{27} + 26x^{18} - 17x^{11} + 7x^3 - 10 = 0$$

(*f*) The set of circles through the origin (0, 0)

1.46. Use Theorem 1.5 to prove Corollary 1.6: If A, B, and C are finite sets, then so is $A \cup B \cup C$ and

$$n(A \cup B \cup C) = n(A) + n(B) + n(C) - n(A \cap B) - n(A \cap C) - n(B \cap C) + n(A \cap B \cap C)$$

1.47. A survey on a sample of 25 new cars being sold at a local auto dealer was conducted to see which of three popular options, air-conditioning (A), radio (R), and power windows (W), were already installed. The survey found:

15 had air-conditioning.
12 had radio.
11 had power windows.
5 had air-conditioning and power windows.
9 had air-conditioning and radio.
4 had radio and power windows.
3 had all three options.

Find the number of cars that had: (*a*) only power windows; (*b*) only air-conditioning; (*c*) only radio; (*d*) radio and power windows but not air-conditioning; (*e*) air-conditioning and radio, but not power windows; and (*f*) only one of the options; (*g*) at least one option; (*h*) none of the options.

CLASSES OF SETS

1.48. Find the power set Power(A) of $A = \{1, 2, 3, 4, 5\}$.

1.49. Given $A = [\{a, b\}, \{c\}, \{d, e, f\}]$.

(a) State whether each of the following is true or false:

(i) $a \in A$, (ii) $\{c\} \subseteq A$, (iii) $\{d, e, f\} \in A$, (iv) $\{\{a, b\}\} \subseteq A$, (v) $\varnothing \subseteq A$.

(b) Find the power set of A.

1.50. Suppose A is a finite set and $n(A) = m$. Prove that Power(A) has 2^m elements.

PARTITIONS

1.51. Let $X = \{1, 2, \ldots, 8, 9\}$. Determine whether or not each of the following is a partition of X:

(a) $[\{1, 3, 6\}, \{2, 8\}, \{5, 7, 9\}]$ (c) $[\{2, 4, 5, 8\}, \{1, 9\}, \{3, 6, 7\}]$

(b) $[\{1, 5, 7\}, \{2, 4, 8, 9\}, \{3, 5, 6\}]$ (d) $[\{1, 2, 7\}, \{3, 5\}, \{4, 6, 8, 9\}, \{3, 5\}]$

1.52. Let $S = \{1, 2, 3, 4, 5, 6\}$. Determine whether or not each of the following is a partition of S:

(a) $P_1 = [\{1, 2, 3\}, \{1, 4, 5, 6\}]$ (c) $P_3 = [\{1, 3, 5\}, \{2, 4\}, \{6\}]$

(b) $P_2 = [\{1, 2\}, \{3, 5, 6\}]$ (d) $P_4 = [\{1, 3, 5\}, \{2, 4, 6, 7\}]$

1.53. Determine whether or not each of the following is a partition of the set **N** of positive integers:

(a) $[\{n: n > 5\}, \{n: n < 5\}]$ (b) $[\{n: n > 5\}, \{0\}, \{1, 2, 3, 4, 5\}]$, ($c$) $[\{n: n^2 > 11\}, \{n: n^2 < 11\}]$

1.54. Let $[A_1, A_2, \ldots, A_m]$ and $[B_1, B_2, \ldots, B_n]$ be partitions of a set X. Show that the collection of sets

$$P = [A_i \cap B_j : i = 1, \ldots, m,\ j = 1, \ldots, n] \backslash \varnothing$$

is also a partition (called the *cross partition*) of X. (Observe that we have deleted the empty set $\varnothing$.)

1.55. Let $X = \{1, 2, 3, \ldots, 8, 9\}$. Find the cross partition P of the following partitions of X:

$$P_1 = [\{1, 3, 5, 7, 9\},\ \{2, 4, 6, 8\}] \quad \text{and} \quad P_2 = [\{1, 2, 3, 4\},\ \{5, 7\},\ \{6, 8, 9\}$$

ARGUMENTS AND VENN DIAGRAMS

1.56. Use a Venn diagram to show that the following argument is valid:

S_1: Babies are illogical.
S_2: Nobody is despised who can manage a crocodile.
S_3: Illogical people are despised.

S: Babies cannot manage crocodiles.

(This argument is adopted from Lewis Carroll, *Symbolic Logic*; he is also the author of *Alice in Wonderland*.)

1.57. Consider the following assumptions:

S_1: All dictionaries are useful.
S_2: Mary owns only romance novels.
S_3: No romance novel is useful.

Determine the validity of each of the following conclusions: (*a*) Romance novels are not dictionaries. (*b*) Mary does not own a dictionary. (*c*) All useful books are dictionaries.

INDUCTION

1.58. Prove: $2 + 4 + 6 + \cdots + 2n = n(n + 1)$.

1.59. Prove: $1 + 4 + 7 + \cdots + (3n - 2) = 2n(3n - 1)$.

1.60. Prove: $\dfrac{1}{1 \cdot 3} + \dfrac{1}{3 \cdot 5} + \dfrac{1}{5 \cdot 7} + \cdots + \dfrac{1}{(2n-1)(2n+1)} = \dfrac{1}{2n+1}$.

1.61. Prove: $1^2 + 2^2 + 3^2 + \ldots + n^2 = \dfrac{n(n+1)(2n+1)}{6}$.

MISCELLANEOUS PROBLEMS

1.62. Suppose $\mathbf{N} = \{1, 2, 3, \ldots\}$ is the universal set and

$A = \{x\colon x \leq 6\}$, $B = \{x\colon 4 \leq x \leq 9\}$, $C = \{1, 3, 5, 7, 9\}$, $D = \{2, 3, 5, 7, 8\}$

Find: (*a*) $A \oplus B$; (*b*) $B \oplus C$; (*c*) $A \cap (B \oplus D)$; (*d*) $(A \cap B) \oplus (A \cap D)$.

1.63. Prove the following properties of the symmetric difference:

(i) $A \oplus (B \oplus C) = (A \oplus B) \oplus C$ (Associative law).
(ii) $A \oplus B = B \oplus A$ (Commutative law).
(iii) If $A \oplus B = A \oplus C$, then $B = C$ (Cancellation law).
(iv) $A \cap (B \oplus C) = (A \cap B) \oplus (A \cap C)$ (Distribution law).

1.64. Consider n distinct sets $A_1, A_2, \ldots, A_n$ in a universal set U. Prove:

(*a*) There are 2^n fundamental products of the n sets.
(*b*) Any two fundamental products are disjoint.
(*c*) U is the union of all the fundamental products.

Answers to Supplementary Problems

1.29. $B = C = E = F$; $A = D = G = H$.

1.30. $A = \{\text{a, e, i, o, u}\}$; $B = D = \{1, \text{i, t, e}\}$; $C = \{\text{a, b, c, d, e}\}$.

1.31. (*a*) C and E; (*b*) D and E; (*c*) A, B, D; (*d*) None.

1.32. (*a*) $A \cap B = \{2, 5\}$; $A \cap C = \{1, 5\}$. (*b*) $A \cup B = \{1, 2, 5, 6, 7\}$; $\mathrm{B} \cup C = \{1, 2, 3, 5, 7, 9\}$.
(*c*) $A^c = \{3, 4, 7, 8, 9\}$; $C^c = \{2, 4, 6, 8\}$.

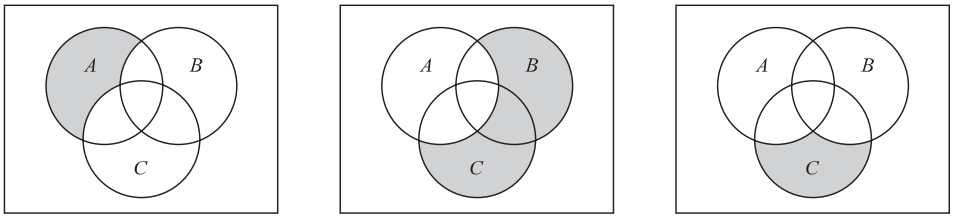
1.33. (*a*) $A\backslash B = \{1, 6\}$; $A\backslash C = \{2, 6\}$. (*b*) $A \oplus B = \{1, 6, 7\}$; $A \oplus C = \{2, 3, 6, 7, 9\}$.

1.34. (*a*) $(A \cup C)\backslash B = \{1, 3, 6, 9\}$. (*b*) $(A \cup B)^c = \{3, 4, 8, 9\}$. (*c*) $(B \oplus C)\backslash A = \{3, 9\}$.

1.35. (*a*) {a, b, c, d, e, f, g}; (*b*) {b, g}; (*c*) {b, c}; (*d*) {a, b, d, e}; (*e*) {a}; (*f*) {a, b, d, e, f, g}; (*g*) {a, d, f}; (*h*) {g}; (*i*) $\varnothing$; (*j*) {c, e, f, g}; (*k*) {a, d, y, h}; (*l*) {c, h}.

1.39. $A \cup B = (A^c \cap B^c)^c$

1.40. See Fig. 1-18.



(*a*) (*b*) (*c*)

Fig. 1-18

1.41. (*a*) $(A \cap B \cap C) \cup (A \cap B \cap C^c) \cup (A \cap B^c \cap C)$
(*b*) $(A^c \cap B \cap C^c) \cup (A^c \cap B \cap C) \cup (A^c \cap B^c \cap C)$
(*c*) $(A \cap B \cap C) \cup (A \cap B \cap C^c) \cup (A \cap B^c \cap C) \cup (A^c \cap B \cap C^c) \cup (A \cap B^c \cap C^c)$

1.42. No such Venn diagram exists. If A and C have an element in common, say x, and $A \subseteq B$; then x must also belong to B. Thus B and C must also have an element in common.

1.43. (*a*) $A \cap B = (B^c \cup A^c)^c$; (*b*) $A = (B^c \cup A) \cap (A \cup B)$; (*c*) $A \cap (A \cup B) = A$; (*d*) $(A \cup B) \cap (A^c \cup B) \cap (A \cup B^c) \cap (A^c \cup B^c) = \varnothing$.

1.45. (*a*) Infinite; (*b*) finite; (*c*) infinite; (*d*) finite; (*e*) finite; (*f*) infinite.

1.47. Use the data to first fill in the Venn diagram of A (air-conditioning), R (radio), and W (power windows) in Fig. 1-19. Then: (*a*) 5; (*b*) 4; (*c*) 2; (*d*) 4; (*e*) 6; (*f*) 11; (*g*) 23; (*h*) 2.

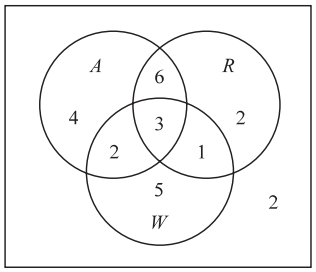


Fig. 1-19

1.48. Power(A) has $2^5 = 32$ elements as follows:
$[\varnothing, \{1\}, \{2\}, \{3\}, \{4\}, \{5\}, \{1,2\}, \{1,3\}, \{1,4\}, \{1,5\}, \{2,3\}, \{2,4\}, \{2,5\}, \{3,4\}, \{3,5\}, \{4,5\}, \{1,2,3\}, \{1,2,4\}, \{1,2,5\}, \{2,3,4\}, \{2,3,5\}, \{3,4,5\}, \{1,3,4\}, \{1,3,5\}, \{1,4,5\}, \{2,4,5\}, \{1,2,3,4\}, \{1,2,3,5\}, \{1,2,4,5\}, \{1,3,4,5\}, \{2,3,4,5\}, A]$.

1.49. (*a*) (i) False; (ii) False; (iii) True; (iv) True; (v) True.
(*b*) Note $n(A) = 3$; hence Power(A) has $2^3 = 8$ elements:

$$\text{Power}(A) = \{A, [\{a,b\}, \{c\}], [\{a,b\}, \{d,e,f\}], [\{c\}, \{d,e,f\}], [\{a,b\}], [\{c\}], [\{d,e,f\}], \varnothing\}$$

1.50. Let x be an arbitrary element in Power(A). For each $a \in A$, there are two possibilities: $a \in A$ or $a \notin A$. But there are m elements in A; hence there are $2 \cdot 2 \cdot \ldots \cdot 2 = 2^m$ different sets X. That is, Power(A) has 2^m elements.

1.51. (*a*) No, (*b*) no, (*c*) yes, (*d*) yes.

1.52. (*a*) No, (*b*) no, (*c*) yes, (*d*) no.

1.53. (*a*) No, (*b*) no, (*c*) yes.

1.55. $P = [\{1,3\}, \{5,7\}, \{9\}, \{2,4\}, \{8\}]$.

1.56. The three premises lead to the Venn diagram in Fig. 1-20. The set of babies and the set of people who can manage crocodiles are disjoint. In other words, the conclusion S is valid.

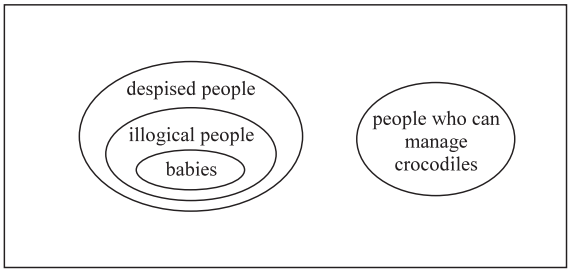


Fig. 1-20

1.57. The three premises lead to the Venn diagram in Fig. 1-21. From this diagram it follows that (*a*) and (*b*) are valid conclusions. However, (*c*) is not a valid conclusion since there may be useful books which are not dictionaries.

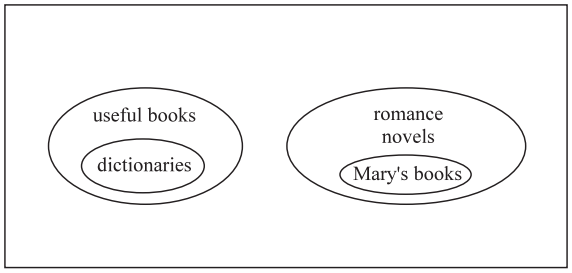


Fig. 1-21

1.62. (*a*) $\{1,2,3,7,8,9\}$; (*b*) $\{1,3,4,6,8\}$; (*c*) $\{2,3,4,6\}$; (*d*) $\{2,3,4,6\}$. [Note (*c*) = (*d*).]

© The McGraw–Hill Companies, 2004

Chapter 2

Relations

2.1 INTRODUCTION

The reader is familiar with many relations which are used in mathematics and computer science, e.g., "less than", "is parallel to", "is a subset of", and so on. In a certain sense, these relations consider the existence or nonexistence of a certain connection between pairs of objects taken in a definite order. Formally, we define a relation in terms of these "ordered pairs".

There are three kinds of relations which play a major role in our theory: (i) equivalence relations, (ii) order relations, (iii) functions. Equivalence relations are mainly covered in this chapter. Order relations are introduced here, but will also be discussed in Chapter 14. Functions are covered in the next chapter.

Relations, as noted above, will be defined in terms of ordered pairs (a, b) of elements, where a is designated as the first element and b as the second element. In particular,

$$(a, b) = (c, d)$$

if and only if $a = c$ and $b = d$. Thus $(a, b) \neq (b, a)$ unless $a = b$. This contrasts with sets studied in Chapter 1, where the order of elements is irrelevant; for example, $\{3, 5\} = \{5, 3\}$.

Although matrices will be covered in Chapter 5, we have included their connection with relations here for completeness. These sections, however, can be ignored at a first reading by those with no previous knowledge of matrix theory.

2.2 PRODUCT SETS

Consider two arbitrary sets A and B. The set of all ordered pairs (a, b) where $a \in A$ and $b \in B$ is called the *product*, or *Cartesian product*, of A and B. A short designation of this product is $A \times B$, which is read "A cross B". By definition,

$$A \times B = \{(a, b) : a \in A \text{ and } b \in B\}$$

One frequently writes A^2 instead of $A \times A$.

EXAMPLE 2.1 $\mathbf{R}$ denotes the set of real numbers and so $\mathbf{R}^2 = \mathbf{R} \times \mathbf{R}$ is the set of ordered pairs of real numbers. The reader is familiar with the geometrical representation of $\mathbf{R}^2$ as points in the plane as in Fig. 2-1. Here each point P represents an ordered pair (a, b) of real numbers and vice versa; the vertical line through P meets the x axis at a, and the horizontal line through P meets the y axis at b. $\mathbf{R}^2$ is frequently called the *Cartesian plane*.

EXAMPLE 2.2 Let $A = \{1, 2\}$ and $B = \{a, b, c\}$. Then

$$A \times B = \{(1, a\}, (1, b), (1, c), (2, a), (2, b), (2, c)\}$$
$$B \times A = \{(a, 1), (a, 2), (b, 1), (b, 2), (c, 1), (c, 2)\}$$

Also $$A \times A = \{(1, 1), (1, 2), (2, 1), (2, 2)\}$$

There are two things worth noting in the above example. First of all $A \times B \neq B \times A$. The Cartesian product deals with ordered pairs, so naturally the order in which the sets are considered is important. Secondly, using $n(S)$ for the number of elements in a set S, we have

$$n(A \times B) = 6 = 2 \cdot 3 = n(A) \cdot n(B)$$

In fact, $n(A \times B) = n(A) \cdot n(B)$ for any finite sets A and B. This follows from the observation that, for an ordered pair (a, b) in $A \times B$, there are $n(A)$ possibilities for a, and for each of these there are $n(B)$ possibilities for b.

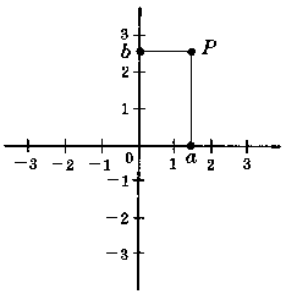


Fig. 2-1

The idea of a product of sets can be extended to any finite number of sets. For any sets $A_1, A_2, \ldots, A_n$, the set of all ordered n-tuples $(a_1, a_2, \ldots, a_n)$ where $a_1 \in A_1$, $a_2 \in A_2, \ldots, a_n \in A_n$ is called the *product* of the sets $A_1, \ldots, A_n$ and is denoted by

$$A_1 \times A_2 \times \cdots \times A_n \qquad \text{or} \qquad \prod_{i=1}^{n} A_i$$

Just as we write A^2 instead of $A \times A$, so we write A^n instead of $A \times A \times \cdots \times A$, where there are n factors all equal to A. For example, $\mathbf{R}^3 = \mathbf{R} \times \mathbf{R} \times \mathbf{R}$ denotes the usual three-dimensional space.

2.3 RELATIONS

We begin with a definition.

Definition. Let A and B be sets. A *binary relation* or, simply, *relation* from A to B is a subset of $A \times B$.

Suppose R is a relation from A to B. Then R is a set of ordered pairs where each first element comes from A and each second element comes from B. That is, for each pair $a \in A$ and $b \in B$, exactly one of the following is true:

(i) $(a, b) \in R$; we than say "a is R-*related* to b", written aRb.

(ii) $(a, b) \notin R$; we then say "a is not R-related to b", written $a \not R b$.

If R is a relation from a set A to itself, that is, if R is a subset of $A^2 = A \times A$, then we say that R is a relation on A.

The *domain* of a relation R is the set of all first elements of the ordered pairs which belong to R, and the *range* of R is the set of second elements.

Although n-ary relations, which involve ordered n-tuples, are introduced in Section 2.12, the term relation shall mean binary relation unless otherwise stated or implied.

EXAMPLE 2.3

(a) Let $A = (1, 2, 3)$ and $B = \{x, y, z\}$, and let $R = \{(1, y), (1, z), (3, y)\}$. Then R is a relation from A to B since R is a subset of $A \times B$. With respect to this relation,

$$1Ry, \quad 1Rz, \quad 3Ry, \qquad \text{but} \qquad 1\not Rx, \quad 2\not Rx, \quad 2\not Ry, \quad 2\not Rz, \quad 3\not Rx, \quad 3\not Rz$$

The domain of R is $\{1, 3\}$ and the range is $\{y, z\}$.

(b) Let $A = \{\text{eggs, milk, corn}\}$ and $B = \{\text{cows, goats, hens}\}$. We can define a relation R from A to B by $(a, b) \in R$ if a is produced by b. In other words,

$$R = \{(\text{eggs, hens}), (\text{milk, cows}), (\text{milk, goats})\}$$

With respect to this relation,

$$\text{eggs } R \text{ hens}, \qquad \text{milk } R \text{ cows}, \qquad \text{etc.}$$

(c) Suppose we say that two countries are *adjacent* if they have some part of their boundaries in common. Then "is adjacent to" is a relation R on the countries of the earth. Thus

$$(\text{Italy, Switzerland}) \in R \qquad \text{but} \qquad (\text{Canada, Mexico}) \notin R$$

(d) Set inclusion $\subseteq$ is a relation on any collection of sets. For, given any pair of sets A and B, either $A \subseteq B$ or $A \not\subseteq B$.

(e) A familiar relation on the set $\mathbf{Z}$ of integers is "m divides n". A common notation for this relation is to write $m|n$ when m divides n. Thus $6|30$ but $7 \not| 25$.

(f) Consider the set L of lines in the plane. Perpendicularity, written $\perp$, is a relation on L. That is, given any pair of lines a and b, either $a \perp b$ or $a \not\perp b$. Similarly, "is parallel to", written $\|$, is a relation on L since either $a \| b$ or $a \not\| b$.

(*g*) Let A be any set. An important relation on A is that of *equality*.

$$\{(a, a): a \in A\}$$

which is usually denoted by "=". This relation is also called the *identity* or *diagonal relation* on A and it will also be denoted by Δ_A or simply Δ.

(*h*) Let A be any set. Then $A \times A$ and $\varnothing$ are subsets of $A \times A$ and hence are relations on A called the *universal relation* and *empty relation*, respectively.

Inverse Relation

Let R be any relation from a set A to a set B. The *inverse* of R, denoted by R^{-1}, is the relation from B to A which consists of those ordered pairs which, when reversed, belong to R; that is,

$$R^{-1} = \{(b, a): (a, b) \in R\}$$

For example, the inverse of the relation $R = \{(1, y), (1, z), (3, y)\}$ from $A = \{1, 2, 3\}$ to $B = \{x, y, z\}$ follows:

$$R^{-1} = \{(y, 1), (z, 1), (y, 3)\}$$

Clearly, if R is any relation, then $(R^{-1})^{-1} = R$. Also, the domain and range of R^{-1} are equal, respectively, to the range and domain of R. Moreover, if R is a relation on A, then R^{-1} is also a relation on A.

2.4 PICTORIAL REPRESENTATIONS OF RELATIONS

First we consider a relation S on the set $\mathbf{R}$ of real numbers; that is, S is a subset of $\mathbf{R}^2 = \mathbf{R} \times \mathbf{R}$.

Since $\mathbf{R}^2$ can be represented by the set of points in the plane, we can picture S by emphasizing those points in the plane which belong to S. The pictorial representation of the relation is sometimes called the *graph* of the relation.

Frequently, the relation S consists of all ordered pairs of real numbers which satisfy some given equation

$$E(x, y) = 0$$

We usually identify the relation with the equation; that is, we speak of the relation $E(x, y) = 0$.

EXAMPLE 2.4 Consider the relation S defined by the equation

$$x^2 + y^2 = 25$$

That is, S consists of all ordered pairs (x, y) which satisfy the given equation. The graph of the equation is a circle having its center at the origin and radius 5. See Fig. 2-2.

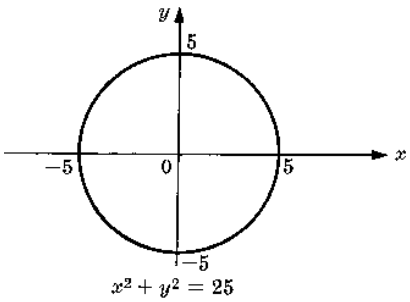


Fig. 2-2

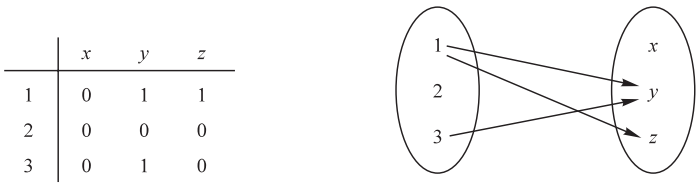
Representations of Relations on Finite Sets

Suppose A and B are finite sets. The following are two ways of picturing a relation R from A to B.

(i) Form a rectangular array whose rows are labeled by the elements of A and whose columns are labeled by the elements of B. Put a 1 or 0 in each position of the array according as $a \in A$ is or is not related to $b \in B$. This array is called the *matrix of the relation*.

(ii) Write down the elements of A and the elements of B in two disjoint disks, and then draw an arrow from $a \in A$ to $b \in B$ whenever a is related to b. This picture will be called the *arrow diagram* of the relation.

Figure 2-3 pictures the first relations in Example 2.3 by the above two ways.



	x	y	z
1	0	1	1
2	0	0	0
3	0	1	0

(i) (ii)

$R = \{(1, y),\ (1, z),\ (3, y)\}$

Fig. 2-3

Directed Graphs of Relations on Sets

There is another way of picturing a relation R when R is a relation from a finite set to itself. First we write down the elements of the set, and then we drawn an arrow from each element x to each element y whenever x is related to y. This diagram is called the *directed graph* of the relation. Figure 2-4, for example, shows the directed graph of the following relation R on the set $A = \{1, 2, 3, 4\}$:

$$R = \{(1,2),\ (2,2),\ (2,4),\ (3,2),\ (3,4),\ (4,1),\ (4,3)\}$$

Observe that there is an arrow from 2 to itself, since 2 is related to 2 under R.

These directed graphs will be studied in detail as a separate subject in Chapter 8. We mention it here mainly for completeness.

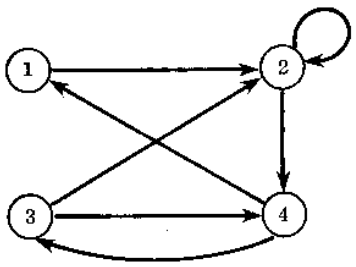


Fig. 2-4

2.5 COMPOSITION OF RELATIONS

Let A, B, and C be sets, and let R be a relation from A to B and let S be a relation from B to C. That is, R is a subset of $A \times B$ and S is a subset of $B \times C$. Then R and S give rise to a relation from A to C denoted by $R \circ S$ and defined by

$$a(R \circ S)c \text{ if for some } b \in B \text{ we have } aRb \text{ and } bSc$$

That is,

$$R \circ S = \{(a, c): \text{there exists } b \in B \text{ for which } (a, b) \in R \text{ and } (b, c) \in S\}$$

The relation $R \circ S$ is called the *composition* of R and S; it is sometimes denoted simply by RS.

Suppose R is a relation on a set A, that is, R is a relation from a set A to itself. Then $R \circ R$, the composition of R with itself is always defined, and $R \circ R$ is sometimes denoted by R^2. Similarly, $R^3 = R^2 \circ R = R \circ R \circ R$, and so on. Thus R^n is defined for all positive n.

Warning: Many texts denote the composition of relations R and S by $S \circ R$ rather than $R \circ S$. This is done in order to conform with the usual use of $g \circ f$ to denote the composition of f and g where f and g are functions. Thus the reader may have to adjust his notation when using this text as a supplement with another text. However, when a relation R is composed with itself, then the meaning of $R \circ R$ is unambiguous.

The arrow diagrams of relations give us a geometrical interpretation of the composition $R \circ S$ as seen in the following example.

EXAMPLE 2.5 Let $A = \{1, 2, 3, 4\}$, $B = \{a, b, c, d\}$, $C = \{x, y, z\}$ and let

$$R = \{(1, a), (2, d), (3, a)\,(3, b), (3, d)\} \quad \text{and} \quad S = \{(b, x), (b, z), (c, y), (d, z)\}$$

Consider the arrow diagrams of R and S as in Fig. 2-5. Observe that there is an arrow from 2 to d which is followed by an arrow from d to z. We can view these two arrows as a "path" which "connects" the element $2 \in A$ to the element $z \in C$. Thus

$$2(R \circ S)z \quad \text{since} \quad 2Rd \text{ and } dSz$$

Similarly there is a path from 3 to x and a path from 3 to z. Hence

$$3(R \circ S)x \quad \text{and} \quad 3(R \circ S)z$$

No other element of A is connected to an element of C. Accordingly,

$$R \circ S = \{(2, z), (3, x), (3, z)\}$$

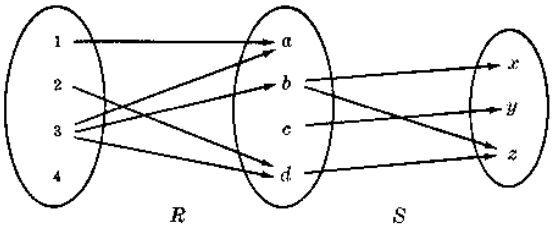


Fig. 2-5

Composition of Relations and Matrices

There is another way of finding $R \circ S$. Let M_R and M_S denote respectively the matrices of the relations R and S. Then

$$M_R = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \end{array} \begin{array}{c} \begin{array}{cccc} a & b & c & d \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \end{array} \qquad \text{and} \qquad M_S = \begin{array}{c} \\ a \\ b \\ c \\ d \end{array} \begin{array}{c} \begin{array}{ccc} x & y & z \end{array} \\ \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \end{array}$$

Multiplying M_R and M_S we obtain the matrix

$$M = M_R M_S = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \end{array} \begin{array}{c} \begin{array}{ccc} x & y & z \end{array} \\ \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix} \end{array}$$

The nonzero entries in this matrix tell us which elements are related by $R \circ S$. Thus $M = M_R M_S$ and $M_{R \circ S}$ have the same nonzero entries.

Our first theorem tells us that the composition of relations is associative.

Theorem 2.1: Let A, B, C and D be sets. Suppose R is a relation from A to B, S is a relation from B to C, and T is a relation from C to D. Then

$$(R \circ S) \circ T = R \circ (S \circ T)$$

We prove this theorem in Problem 2.11.

2.6 TYPES OF RELATIONS

Consider a given set A. This section discusses a number of important types of relations which are defined on A.

Reflexive Relations

A relation R on a set A is *reflexive* if aRa for every $a \in A$, that is, if $(a, a) \in R$ for every $a \in A$. Thus R is not reflexive if there exists an $a \in A$ such that $(a, a) \notin R$.

EXAMPLE 2.6 Consider the following five relations on the set $A = \{1, 2, 3, 4\}$:

$R_1 = \{(1,1), (1,2), (2,3), (1,3), (4,4)\}$
$R_2 = \{(1,1), (1,2), (2,1), (2,2), (3,3), (4,4)\}$
$R_3 = \{(1,3), (2,1)\}$
$R_4 = \varnothing$, the empty relation
$R_5 = A \times A$, the universal relation

Determine which of the relations are reflexive.

Since A contain the four elements 1, 2, 3, and 4, a relation R on A is reflexive if it contains the four pairs (1, 1), (2, 2), (3, 3), and (4, 4). Thus only R_2 and the universal relation $R_5 = A \times A$ are reflexive. Note that R_1, R_3, and R_4 are not reflexive since, for example, (2, 2) does not belong to any of them.

EXAMPLE 2.7 Consider the following five relations:

(1) Relation $\leq$ (less than or equal) on the set $\mathbf{Z}$ of integers
(2) Set inclusion $\subseteq$ on a collection $\mathcal{C}$ of sets
(3) Relation $\perp$ (perpendicular) on the set L of lines in the plane.
(4) Relation $\parallel$ (parallel) on the set L of lines in the plane.
(5) Relation $|$ of divisibility on the set $\mathbf{N}$ of positive integers. (Recall $x|y$ if there exists z such that $xz = y$.)

Determine which of the relations are reflexive.

The relation (3) is not reflexive since no line is perpendicular to itself. Also (4) is not reflexive since no line is parallel to itself. The other relations are reflexive; that is, $x \leq x$ for every integer x in $\mathbf{Z}$, $A \subseteq A$ for any set A in $\mathcal{C}$, and $n|n$ for every positive integer n in $\mathbf{N}$.

Symmetric and Antisymmetric Relations

A relation R on a set A is *symmetric* if whenever aRb then bRa, that is, if whenever $(a, b) \in R$ then $(b, a) \in R$. Thus R is not symmetric if there exists $a, b \in A$ such that $(a, b) \in R$ but $(b, a) \notin R$.

EXAMPLE 2.8

(*a*) Determine which of the relations in Example 2.6 are symmetric.

R_1 is not symmetric since $(1, 2) \in R_1$ but $(2, 1) \notin R_1$. R_3 is not symmetric since $(1, 3) \in R_3$ but $(3, 1) \notin R_3$. The other relations are symmetric.

(*b*) Determine which of the relations in Example 2.7 are symmetric.

The relation $\perp$ is symmetric since if line a is perpendicular to line b then b is perpendicular to a. Also, $\parallel$ is symmetric since if line a is parallel to line b then b is parallel to a. The other relations are not symmetric. For example, $3 \leq 4$ but $4 \not\leq 3$; $\{1, 2\} \subseteq \{1, 2, 3\}$ but $\{1, 2, 3\} \not\subseteq \{1, 2\}$, and $2|6$ but $6 \not| 2$.

A relation R on a set A is *antisymmetric* if whenever aRb and bRa then $a = b$, that is, if whenever $(a, b), (b, a) \in R$ then $a = b$. Thus R is not antisymmetric if there exist $a, b \in A$ such that (a, b) and (b, a) belong to R, but $a \neq b$.

EXAMPLE 2.9

(*a*) Determine which of the relations in Example 2.6 are antisymmetric.

R_2 is not antisymmetric since (1, 2) and (2, 1) belong to R_2, but $1 \neq 2$. Similarly, the universal relation R_5 is not antisymmetric. All the other relations are antisymmetric.

(*b*) Determine which of the relations in Example 2.7 are antisymmetric.

The relation $\leq$ is antisymmetric since whenever $a \leq b$ and $b \leq a$ then $a = b$. Set inclusion $\subseteq$ is antisymmetric since whenever $A \subseteq B$ and $B \subseteq A$ then $A = B$. Also, divisibility on $\mathbf{N}$ is antisymmetric since whenever $m|n$ and $n|m$ then $m = n$. (Note that divisibility on $\mathbf{Z}$ is not antisymmetric since $3| -3$ and $-3|3$ but $3 \neq -3$.) The relation $\perp$ is not antisymmetric since we can have distinct lines a and b such that $a \perp b$ and $b \perp a$. Similarly, $\parallel$ is not antisymmetric.

Remark: The properties of being symmetric and being antisymmetric are not negatives of each other. For example, the relation $R = \{(1, 3), (3, 1), (2, 3)\}$ is neither symmetric nor antisymmetric. On the other hand, the relation $R' = \{(1, 1), (2, 2)\}$ is both symmetric and antisymmetric.

Transitive Relations

A relation R on a set A is *transitive* if whenever aRb and bRc then aRc, that is, if whenever $(a, b), (b, c) \in R$ then $(a, c) \in R$. Thus R is not transitive if there exist $a, b, c \in A$ such that $(a, b), (b, c) \in R$ but $(a, c) \notin R$.

EXAMPLE 2.10

(*a*) Determine which of the relations in Example 2.6 are transitive.

The relation R_3 is not transitive since $(2, 1), (1, 3) \in R_3$ but $(2, 3) \notin R_3$. All the other relations are transitive.

(*b*) Determine which of the relations in Example 2.7 are transitive.

The relations $\leq$, $\subseteq$, and $|$ are transitive. That is: (i) If $a \leq b$ and $b \leq c$, then $a \leq c$. (ii) If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$. (iii) If $a|b$ and $b|c$, then $a|c$,

On the other hand the relation $\perp$ is not transitive. If $a \perp b$ and $b \perp c$, then it is not true that $a \perp c$. Since no line is parallel to itself, we can have $a \parallel b$ and $b \parallel a$, but $a \nparallel a$. Thus $\parallel$ is not transitive. (We note that the relation "is parallel or equal to" is a transitive relation on the set L of lines in the plane.)

The property of transitivity can also be expressed in terms of the composition of relations. For a relation R on A we define

$$R^2 = R \circ R \qquad \text{and, more generally,} \qquad R^n = R^{n-1} \circ R$$

Then we have the following result.

Theorem 2.2: A relation R is transitive if and only if $R^n \subseteq R$ for $n \geq 1$.

2.7 CLOSURE PROPERTIES

Consider a given set A and the collection of all relations on A. Let P be a property of such relations, such as being symmetric or being transitive. A relation with property P will be called a P-relation. The *P-closure* of an arbitrary relation R on A, written $P(R)$, is a P-relation such that

$$R \subseteq P(R) \subseteq S$$

for every P-relation S containing R. We will write

$$\text{reflexive}(R), \qquad \text{symmetric}(R), \qquad \text{and transitive}(R)$$

for the reflexive, symmetric, and transitive closures of R.

Generally speaking, $P(R)$ need not exist. However, there is a general situation where $P(R)$ will always exist. Suppose P is a property such that there is at least one P-relation containing R and that the intersection of any P-relations is again a P-relation. Then one can prove (Problem 2.16) that

$$P(R) = \cap(S\text{: } S \text{ is a } P\text{-relation and } R \subseteq S)$$

Thus one can obtain $P(R)$ from the "top-down", that is, as the intersection of relations. However, one usually wants to find $P(R)$ from the "bottom-up", that is, by adjoining elements to R to obtain $P(R)$. This we do below.

Reflexive and Symmetric Closures

The next theorem tells us how to easily obtain the reflexive and symmetric closures of a relation. Here $\Delta_A = \{(a, a)\text{: } a \in A\}$ is the *diagonal* or *equality* relation on A.

Theorem 2.3: Let R be a relation on a set A. Then:

(i) $R \cup \Delta_A$ is the reflexive closure of R.

(ii) $R \cup R^{-1}$ is the symmetric closure of R.

In other words, reflexive(R) is obtained by simply adding to R those elements (a, a) in the diagonal which do not already belong to R, and symmetric(R) is obtained by adding to R all pairs (b, a) whenever (a, b) belongs to R.

EXAMPLE 2.11

(*a*) Consider the following relation R on the set $A = \{1, 2, 3, 4\}$:

$$R = \{(1,1),\ (1,3),\ (2,4),\ (3,1),\ (3,3),\ (4,3)\}$$

Then

$$\text{reflexive}(R) = R \cup \{(2,2),\ (4,4)\} \qquad \text{and} \qquad \text{symmetric}(R) = R \cup \{(4,2),\ (3,4)\}$$

(*b*) Consider the relation $<$ (less than) on the set **N** of positive integers. Then

$$\text{reflexive}(<) = < \cup \Delta = \leq = \{(a, b): a \leq b\}$$

$$\text{symmetric}(<) = < \cup > = \{(a, b): a \neq b\}$$

Transitive Closure

Let R be a relation on a set A. Recall that $R^2 = R \circ R$ and $R^n = R^{n-1} \circ R$. We define

$$R^* = \bigcup_{i=1}^{\infty} R^i$$

The following theorem applies.

Theorem 2.4: R^* is the transitive closure of a relation R.

Suppose A is a finite set with n elements. Then we show in Chapter 8 on directed graphs that

$$R^* = R \cup R^2 \cup \cdots \cup R^n$$

This gives us the following result.

Theorem 2.5: Let R be a relation on a set A with n elements. Then

$$\text{transitive}(R) = R \cup R^2 \cup \cdots \cup R^n$$

Finding transitive(R) can take a lot of time when A has a large number of elements. An efficient way for doing this will be described in Chapter 8. Here we give a simple example where A has only three elements.

EXAMPLE 2.12 Consider the following relation R on $A = \{1, 2, 3\}$:

$$R = \{(1, 2), (2, 3), (3, 3)\}$$

Then

$$R^2 = R \circ R = \{(1, 3), (2, 3)(3, 3)\} \qquad \text{and} \qquad R^3 = R^2 \circ R = \{(1, 3), (2, 3), (3, 3)\}$$

Accordingly,

$$\text{transitive}(R) = R \cup R^2 \cup R^3 = \{(1, 2), (2, 3), (3, 3), (1, 3)\}$$

2.8 EQUIVALENCE RELATIONS

Consider a nonempty set S. A relation R on S is an *equivalence relation* if R is reflexive, symmetric, and transitive. That is, R is an equivalence relation on S if it has the following three properties:

(1) For every $a \in S$, aRa.
(2) If aRb, then bRa.
(3) If aRb and bRc, then aRc.

The general idea behind an equivalence relation is that it is a classification of objects which are in some way "alike". In fact, the relation "=" of equality on any set S is an equivalence relation; that is:

(1) $a = a$ for every $a \in S$.
(2) If $a = b$, then $b = a$.
(3) If $a = b$ and $b = c$, then $a = c$.

Other equivalence relations follow.

EXAMPLE 2.13

(*a*) Consider the set L of lines and the set T of triangles in the Euclidean plane. The relation "is parallel to or identical to" is an equivalence relation on L, and congruence and similarity are equivalence relations on T.

(*b*) The classification of animals by species, that is, the relation "is of the same species as", is an equivalence relation on the set of animals.

(*c*) The relation $\subseteq$ of set inclusion is not an equivalence relation. It is reflexive and transitive, but it is not symmetric since $A \subseteq B$ does not imply $B \subseteq A$.

(*d*) Let m be a fixed positive integer. Two integers a and b are said to be *congruent modulo* m, written

$$a \equiv b \pmod{m}$$

if m divides $a - b$. For example, for $m = 4$ we have $11 \equiv 3 \pmod 4$ since 4 divides $11 - 3$, and $22 \equiv 6 \pmod 4$ since 4 divides $22 - 6$. This relation of congruence modulo m is an equivalence relation.

Equivalence Relations and Partitions

This subsection explores the relationship between equivalence relations and partitions on a nonempty set S. Recall first that a partition P of S is a collection $\{A_i\}$ of nonempty subsets of S with the following two properties:

(1) Each $a \in S$ belongs to some A_i.
(2) If $A_i \neq A_j$, then $A_i \cap A_j = \varnothing$.

In other words, a partition P of S is a subdivision of S into disjoint nonempty sets. (See Section 1.9.)

Suppose R is an equivalence relation on a set S. For each a in S, let $[a]$ denote the set of elements of S to which a is related under R; that is,

$$[a] = \{x\colon (a, x) \in R\}$$

We call $[a]$ the *equivalence class* of a in S; any $b \in [a]$ is called a *representative* of the equivalence class.

The collection of all equivalence classes of elements of S under an equivalence relation R is denoted by S/R, that is,

$$S/R = \{[a]\colon a \in S\}$$

It is called the *quotient* set of S by R. The fundamental property of a quotient set is contained in the following theorem.

Theorem 2.6: Let R be an equivalence relation on a set S. Then the quotient set S/R is a partition of S. Specifically:

(i) For each a in S, we have $a \in [a]$.
(ii) $[a] = [b]$ if and only if $(a, b) \in R$.
(iii) If $[a] \neq [b]$, then $[a]$ and $[b]$ are disjoint.

Conversely, given a partition $\{A_i\}$ of the set S, there is an equivalence relation R on S such that the sets A_i are the equivalence classes.

This important theorem will be proved in Problem 2.21.

EXAMPLE 2.14

(*a*) Consider the following relation R on $S = \{1, 2, 3\}$:

$$R = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 3)\}$$

One can show that R is reflexive, symmetric, and transitive, that is, that R is an equivalence relation. Under the relation R,

$$[1] = \{1, 2\}, \qquad [2] = \{1, 2\}, \qquad [3] = \{3\}$$

Observe that $[1] = [2]$ and that $S/R = \{[1], [3]\}$ is a partition of S. One can choose either $\{1, 3\}$ or $\{2, 3\}$ as a set of representatives of the equivalence classes.

(*b*) Let R_5 be the relation on the set $\mathbf{Z}$ of integers defined by

$$x \equiv y \pmod 5$$

which reads "x is congruent to y modulo 5" and which means that the difference $x - y$ is divisible by 5. Then R_5 is an equivalence relation on $\mathbf{Z}$. There are exactly five equivalence classes in the quotient set $\mathbf{Z}/R_5$ as follows:

$$\begin{aligned} A_0 &= \{\ldots, -10, -5, 0, 5, 10, \ldots\} \\ A_1 &= \{\ldots, -9, -4, 1, 6, 11, \ldots\} \\ A_2 &= \{\ldots, -8, -3, 2, 7, 12, \ldots\} \\ A_3 &= \{\ldots, -7, -2, 3, 8, 13, \ldots\} \\ A_4 &= \{\ldots, -6, -1, 4, 9, 14, \ldots\} \end{aligned}$$

Observe that any integer x, which can be uniquely expressed in the form $x = 5q + r$ where $0 \leq r < 5$, is a member of the equivalence class A_r where r is the remainder. As expected, the equivalence classes are disjoint and

$$\mathbf{Z} = A_0 \cup A_1 \cup A_2 \cup A_3 \cup A_4$$

Usually one chooses $\{0, 1, 2, 3, 4\}$ or $\{-2, -1, 0, 1, 2\}$ as a set of representatives of the equivalence classes.

2.9 PARTIAL ORDERING RELATIONS

This section defines another important class of relations. A relation R on a set S is called a *partial ordering* or a *partial order* if R is reflexive, antisymmetric, and transitive. A set S together with a partial ordering R is called a *partially ordered set* or *poset*. Partially ordered sets will be studied in more detail in Chapter 14, so here we simply give some examples.

EXAMPLE 2.15

(*a*) The relation $\subseteq$ of set inclusion is a partial ordering on any collection of sets since set inclusion has the three desired properties. That is,

(1) $A \subseteq A$ for any set A.
(2) If $A \subseteq B$ and $B \subseteq A$, then $A = B$.
(3) If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

(*b*) The relation $\leq$ on the set $\mathbf{R}$ of real numbers is reflexive, antisymmetric, and transitive. Thus $\leq$ is a partial ordering.

(*c*) The relation "a divides b" is a partial ordering on the set $\mathbf{N}$ of positive integers. However, "a divides b" is not a partial ordering on the set $\mathbf{Z}$ of integers since $a|b$ and $b|a$ does not imply $a = b$. For example, $3| - 3$ and $-3|3$ but $3 \neq -3$.

2.10 *n*-ARY RELATIONS

All the relations discussed above were binary relations. By an *n-ary relation*, we mean a set of ordered n-tuples. For any set S, a subset of the product set S^n is called an n-ary relation on S. In particular, a subset of S^3 is called a *ternary relation* on S.

EXAMPLE 2.16

(*a*) Let L be a line in the plane. Then "betweenness" is a ternary relation R on the points of L; that is, $(a, b, c) \in R$ if b lies between a and c on L.

(*b*) The equation $x^2 + y^2 + z^2 = 1$ determines a ternary relation T on the set $\mathbf{R}$ of real numbers. That is, a triple (x, y, z) belongs to T if (x, y, z) satisfies the equation, which means (x, y, z) is the coordinates of a point in $\mathbf{R}^3$ on the sphere S with radius 1 and center at the origin $O = (0, 0, 0)$.

Solved Problems

ORDERED PAIRS AND PRODUCT SETS

2.1. Given: $A = \{1, 2, 3\}$ and $B = \{a, b\}$. Find: (*a*) $A \times B$; (*b*) $B \times A$; (*c*) $B \times B$.

(*a*) $A \times B$ consists of all ordered pairs (x, y) where $x \in A$ and $y \in B$. Hence

$$A \times B = \{(1, a), (1, b), (2, a), (2, b), (3, a), (3, b)\}$$

(*b*) $B \times A$ consists of all ordered pairs (y, x) where $y \in B$ and $x \in A$. Hence

$$B \times A = \{(a, 1), (a, 2), (a, 3), (b, 1), (b, 2), (b, 3)\}$$

(*c*) $B \times B$ consists of all ordered pairs (x, y) where $x, y \in B$. Hence

$$B \times B = \{(a, a), (a, b), (b, a), (b, b)\}$$

As expected, the number of elements in the product set is equal to the product of the numbers of the elements in each set.

2.2. Given: $A = \{1, 2\}, B = \{x, y, z\}$, and $C = \{3, 4\}$. Find: $A \times B \times C$.

$A \times B \times C$ consists of all ordered triplets (a, b, c) where $a \in A$, $b \in B$, $c \in C$. These elements of $A \times B \times C$ can be systematically obtained by a so-called tree diagram (Fig. 2-6). The elements of $A \times B \times C$ are precisely the 12 ordered triplets to the right of the tree diagram.

Observe that $n(A) = 2$, $n(B) = 3$, and $n(C) = 2$ and, as expected,

$$n(A \times B \times C) = 12 = n(A) \cdot n(B) \cdot n(C)$$

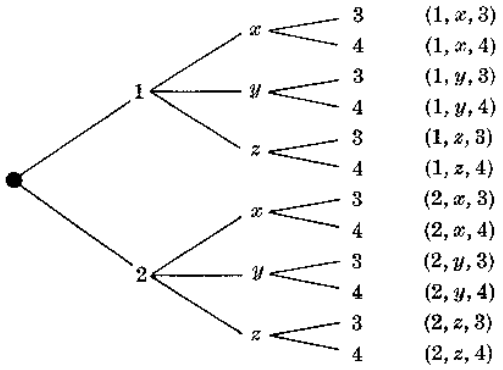


Fig. 2-6

2.3. Let $A = \{1, 2\}, B = \{a, b, c\}$ and $C = \{c, d\}$. Find: $(A \times B) \cap (A \times C)$ and $(B \cap C)$.

We have

$$A \times B = \{(1, a), (1, b), (1, c), (2, a), (2, b), (2, c)\}$$
$$A \times C = \{(1, c), (1, d), (2, c), (2, d)\}$$

Hence

$$(A \times B) \cap (A \times C) = \{(1, c), (2, c)\}$$

Since $B \cap C = \{c\}$,

$$A \times (B \cap C) = \{(1, c), (2, c)\}$$

Observe that $(A \times B) \cap (A \times C) = A \times (B \cap C)$. This is true for any sets A, B and C (see Problem 2.4).

2.4. Prove $(A \times B) \cap (A \times C) = A \times (B \cap C)$.

$$\begin{aligned}(A \times B) \cap (A \times C) &= \{x, y)\colon (x, y) \in A \times B \text{ and } (x, y) \in A \times C\} \\ &= \{(x, y)\colon x \in A, y \in B \text{ and } x \in A, y \in C\} \\ &= \{(x, y)\colon x \in A, y \in B \cap C\} \quad = \quad A \times (B \cap C)\end{aligned}$$

2.5. Find x and y given $(2x, x + y) = (6, 2)$.

Two ordered pairs are equal if and only if the corresponding components are equal. Hence we obtain the equations

$$2x = 6 \qquad \text{and} \qquad x + y = 2$$

from which we derive the answers $x = 3$ and $y = -1$.

RELATIONS AND THEIR GRAPHS

2.6. Find the number of relations from $A = \{a, b, c\}$ to $B = \{1, 2\}$.

There are $3(2) = 6$ elements in $A \times B$, and hence there are $m = 2^6 = 64$ subsets of $A \times B$. Thus there are $m = 64$ relations from A to B.

2.7. Given $A = \{1, 2, 3, 4\}$ and $B = \{x, y, z\}$. Let R be the following relation from A to B:

$$R = \{(1, y), (1, z), (3, y), (4, x), (4, z)\}$$

(*a*) Determine the matrix of the relation.

(*b*) Draw the arrow diagram of R.

(*c*) Find the inverse relation R^{-1} of R.

(*d*) Determine the domain and range of R.

(*a*) See Fig. 2-7(*a*). Observe that the rows of the matrix are labeled by the elements of A and the columns by the elements of B. Also observe that the entry in the matrix corresponding to $a \in A$ and $b \in B$ is 1 if a is related to b and 0 otherwise.

(*b*) See Fig. 2-7(*b*). Observe that there is an arrow from $a \in A$ to $b \in B$ iff a is related to b, i.e., iff $(a, b) \in R$.

(*c*) Reverse the ordered pairs of R to obtain R^{-1}:

$$R^{-1} = \{(y, 1), (z, 1), (y, 3), (x, 4), (z, 4)\}$$

Observe that by reversing the arrows in Fig. 2.7(*b*) we obtain the arrow diagram of R^{-1}.

(*d*) The domain of R, $\mathrm{Dom}(R)$, consists of the first elements of the ordered pairs of R, and the range of R. $\mathrm{Ran}(R)$, consists of the second elements. Thus,

$$\mathrm{Dom}(R) = \{1, 3, 4\} \qquad \text{and} \qquad \mathrm{Ran}(R) = \{x, y, z\}$$

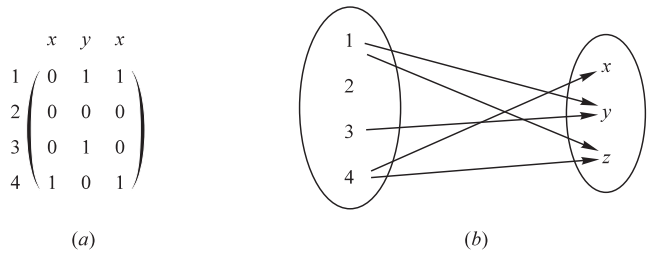


Fig. 2-7

2.8. Let $A = \{1, 2, 3, 4, 6\}$, and let R be the relation on A defined by "x divides y", written $x|y$. (Note $x|y$ iff there exists an integer z such that $x\,z = y$.)

(*a*) Write R as a set of ordered pairs.

(*b*) Draw its directed graph.

(*c*) Find the inverse relation R^{-1} of R. Can R^{-1} be described in words?

(*a*) Find those numbers in A divisible by 1, 2, 3, 4, and then 6. These are:

$$1|1, \quad 1|2, \quad 1|3, \quad 1|4, \quad 1|6, \quad 2|2, \quad 2|4, \quad 2|6, \quad 3|3, \quad 3|6, \quad 4|4, \quad 6|6$$

Hence

$$R = \{(1,1), (1,2), (1,3), (1,4), (1,6), (2,2), (2,4), (2,6), (3,3), (3,6), (4,4), (6,6)\}$$

(*b*) See Fig. 2-8.

(*c*) Reverse the ordered pairs of R to obtain R^{-1}:

$$R^{-1} = \{(1,1), (2,1), (3,1), (4,1), (6,1), (2,2), (4,2), (6,2), (3,3), (6,3), (4,4), (6,6)\}$$

R^{-1} can be described by the statement "x is a multiple of y".

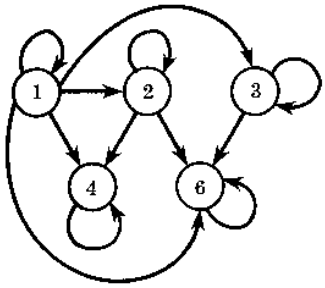


Fig. 2-8

2.9. Let $A = \{1, 2, 3\}$, $B = \{a, b, c\}$, and $C = \{x, y, z\}$. Consider the following relations R and S from A to B and from B to C, respectively.

$$R = \{(1, b), (2, a), (2, c)\} \qquad \text{and} \qquad S = \{(a, y), (b, x), (c, y), (c, z)\}$$

(*a*) Find the composition relation $R \circ S$.

(*b*) Find the matrices M_R, M_S, and $M_{R\circ S}$ of the respective relations R, S, and $R \circ S$, and compare $M_{R\circ S}$ to the product $M_R M_S$.

(*a*) Draw the arrow diagram of the relations R and S as in Fig. 2-9. Observe that 1 in A is "connected" to x in C by the path $1 \to b \to x$; hence $(1, x)$ belongs to $R \circ S$. Similarly, $(2, y)$ and $(2, z)$ belong to $R \circ S$. We have

$$R \circ S = \{(1, x), (2, y), (2, z)\}$$

(See Example 2.5.)

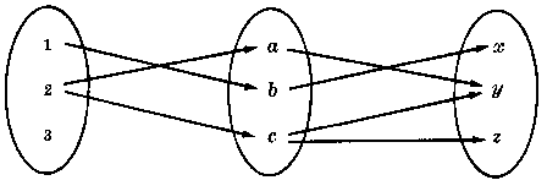


Fig. 2-9

(*b*) The matrices of M_R, M_S, and $M_{R\circ S}$ follow:

$$M_R = \begin{array}{c} \\ 1 \\ 2 \\ 3 \end{array}\!\!\begin{array}{c} \begin{array}{ccc} a & b & c \end{array} \\ \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \end{array} \qquad M_S = \begin{array}{c} \\ a \\ b \\ c \end{array}\!\!\begin{array}{c} \begin{array}{ccc} x & y & z \end{array} \\ \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix} \end{array} \qquad M_{R\circ S} = \begin{array}{c} \\ 1 \\ 2 \\ 3 \end{array}\!\!\begin{array}{c} \begin{array}{ccc} x & y & z \end{array} \\ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix} \end{array}$$

Multiplying M_R and M_S we obtain

$$M_R M_S = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

Observe that $M_{R\circ S}$ and $M_R M_S$ have the same zero entries.

2.10. Let R and S be the following relations on $A = \{1, 2, 3\}$:

$$R = \{(1, 1), (1, 2), (2, 3), (3, 1), (3, 3)\}, \qquad S = \{(1, 2), (1, 3), (2, 1), (3, 3)\}$$

Find (*a*) $R \cap S, R \cup S, R^c$; (*b*) $R \circ S$; (*c*) $S^2 = S \circ S$.

(*a*) Treat R and S simply as sets, and take the usual intersection and union. For R^c, use the fact that $A \times A$ is the universal relation on A.

$$R \cap S = \{(1, 2), (3, 3)\}$$
$$R \cup S = \{(1, 1), (1, 2), (1, 3), (2, 1), (2, 3), (3, 1), (3, 3)\}$$
$$R^c = \{(1, 3), (2, 1), (2, 2), (3, 2)\}$$

(*b*) For each pair $(a, b) \in R$, find all pairs $(b, c) \in S$. Then $(a, c) \in R \circ S$. For example, $(1, 1) \in R$ and $(1, 2), (1, 3) \in S$; hence $(1, 2)$ and $(1, 3)$ belong to $R \circ S$. Thus,

$$R \circ S = \{(1, 2), (1, 3), (1, 1), (2, 3), (3, 2), (3, 3)$$

(*c*) Following the algorithm in (*b*), we get

$$S^2 = S \circ S = \{(1, 1), (1, 3), (2, 2), (2, 3), (3, 3)\}$$

2.11. Prove Theorem 2.1: Let A, B, C and D be sets. Suppose R is a relation from A to B, S is a relation from B to C and T is a relation from C to D. Then $(R \circ S) \circ T = R \circ (S \circ T)$.

We need to show that each ordered pair in $(R \circ S) \circ T$ belongs to $R \circ (S \circ T)$, and vice versa.

Suppose (a, d) belongs to $(R \circ S) \circ T$. Then there exists a c in C such that $(a, c) \in R \circ S$ and $(c\,d) \in T$. Since $(a, c) \in R \circ S$, there exists a b in B such that $(a, b) \in R$ and $(b, c) \in S$. Since $(b, c) \in S$ and $(c, d) \in T$, we have $(b, d) \in S \circ T$; and since $(a, b) \in R$ and $(b, d) \in S \circ T$, we have $(a, d) \in R \circ (S \circ T)$. Therefore, $(R \circ S) \circ T \subseteq R \circ (S \circ T)$. Similarly $R \circ (S \circ T) \subseteq (R \circ S) \circ T$. Both inclusion relations prove $(R \circ S) \circ T = R \circ (S \circ T)$.

TYPES OF RELATIONS AND CLOSURE PROPERTIES

2.12. Consider the following five relations on the set $A = \{1, 2, 3\}$:

$$R = \{(1,1), (1,2), (1,3), (3,3)\} \qquad \varnothing = \text{empty relation}$$
$$S = \{(1,1), (1,2), (2,1), (2,2), (3,3) \qquad A \times A = \text{universal relation}$$
$$T = \{(1,1), (1,2), (2,2), (2,3)\}$$

Determine whether or not each of the above relations on A is: (*a*) reflexive; (*b*) symmetric; (*c*) transitive; (*d*) antisymmetric.

(*a*) R is not reflexive since $2 \in A$ but $(2, 2) \notin R$. T is not reflexive since $(3, 3) \notin T$ and, similarly, $\varnothing$ is not reflexive. S and $A \times A$ are reflexive.

(*b*) R is not symmetric since $(1, 2) \in R$ but $(2, 1) \notin R$, and similarly T is not symmetric. S, $\varnothing$, and $A \times A$ are symmetric.

(*c*) T is not transitive since $(1, 2)$ and $(2, 3)$ belong to T, but $(1, 3)$ does not belong to T. The other four relations are transitive.

(*d*) S is not antisymmetric since $1 \neq 2$, and $(1, 2)$ and $(2, 1)$ both belong to S. Similarly, $A \times A$ is not antisymmetric. The other three relations are antisymmetric.

2.13. Given $A = \{1, 2, 3, 4\}$. Consider the following relation in A:

$$R = \{(1,1), (2,2), (2,3), (3,2), (4,2), (4,4)\}$$

(*a*) Draw its directed graph.

(*b*) Is R (i) reflexive, (ii) symmetric, (iii) transitive, or (iv) antisymmetric?

(*c*) Find $R^2 = R \circ R$.

(*a*) See Fig. 2-10.

(*b*) (i) R is not reflexive because $3 \in A$ but $3 \not R 3$, i.e., $(3, 3) \notin R$.

(ii) R is not symmetric because $4R2$ but $2 \not R 4$, i.e., $(4, 2) \in R$ but $(2, 4) \notin R$.

(iii) R is not transitive because $4R2$ and $2R3$ but $4 \not R 3$, i.e., $(4, 2) \in R$ and $(2, 3) \in R$ but $(4, 3) \notin R$.

(iv) R is not antisymmetric because $2R3$ and $3R2$ but $2 \neq 3$.

(*c*) For each pair $(a, b) \in R$, find all $(b, c) \in R$. Since $(a, c) \in R^2$,

$$R^2 = \{(1,1), (2,2), (2,3), (3,2), (3,3), (4,2), (4,3), (4,4)\}$$

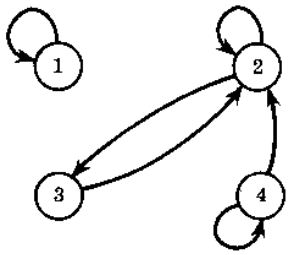


Fig. 2-10

2.14. Give examples of relations R on $A = \{1, 2, 3\}$ having the stated property.

(a) R is both symmetric and antisymmetric.

(b) R is neither symmetric nor antisymmetric.

(c) R is transitive but $R \cup R^{-1}$ is not transitive.

There are several possible examples for each answer. One possible set of examples follows:

(a) $R = \{(1, 1), (2, 2)\}$.

(b) $R = \{(1, 2), (2, 1), (2, 3)\}$.

(c) $R = \{1, 2)\}$.

2.15. Suppose C is a collection of relations S on a set A and let T be the intersection of the relation S, that is, $T = \cap(S: S \in C)$. Prove:

(a) If every S is symmetric, then T is symmetric.

(b) If every S is transitive, then T is transitive.

(a) Suppose $(a, b) \in T$. Then $(a, b) \in S$ for every S. Since each S is symmetric, $(b, a) \in S$ for every S. Hence $(b, a) \in T$ and T is symmetric.

(b) Suppose (a, b) and (b, c) belong to T. Then (a, b) and (b, c) belong to S for every S. Since each S is transitive, (a, c) belongs to S for every S. Hence, $(a, c) \in T$ and T is transitive.

2.16. Let R be a relation on a set A, and let P be a property of relations, such as, symmetry and transitivity. Then P will be called R-closable if P satisfies the following two conditions:

(1) There is a P-relation S containing R.

(2) The intersection of P-relations is a P-relation.

(a) Show that symmetry and transitivity are R-closable for any relation R.

(b) Suppose P is R-closable. Then $P(R)$, the P-closure of R, is the intersection of all P-relations S containing R, that is,

$$P(R) = \cap(S: S \text{ is a } P\text{-relation and } R \subseteq S)$$

(a) The universal relation $A \times A$ is symmetric and transitive and $A \times A$ contains any relation R on A. Thus (1) is satisfied. By Problem 2.15, symmetry and transitivity satisfy (2). Thus symmetry and transivity are R-closable for any relation R.

(b) Let $T = \cap(S: S \text{ is a } P\text{-relation and } R \subseteq S)$. Since P is R-closable, T is nonempty by (1) and T is a P-relation by (2). Since each relation S contains R, the intersection T contains R. Thus, T is a P-relation containing R. By definition, $P(R)$ is the smallest P-relation containing R; hence $P(R) \subseteq T$. On the

other hand, $P(R)$ is one of the sets S defining T, that is, $P(R)$ is a P-relation and $R \subseteq P(R)$. Therefore, $T \subseteq P(R)$. Accordingly, $P(R) = T$.

2.17. Consider a set $A = \{a, b, c\}$ and the relation R on A defined by

$$R = \{(a, a),\ (a, b),\ (b, c),\ (c, c)\}$$

Find (*a*) reflexive(R); (*b*) symmetric(R); and (*c*) transitive(R).

(*a*) The reflexive closure on R is obtained by adding all diagonal pairs of $A \times A$ to R which are not currently in R. Hence,

$$\text{reflexive}(R) = R \cup \{(b, b)\} = \{(a, a), (a, b), (b, b), (b, c), (c, c)\}$$

(*b*) The symmetric closure on R is obtained by adding all the pairs in R^{-1} to R which are not currently in R. Hence,

$$\text{symmetric}(R) = R \cup \{(b, a), (c, b)\} = \{(a, a), (a, b), (b, a), (b, c), (c, b), (c, c)\}$$

(*c*) The transitive closure on R, since A has three elements, is obtained by taking the union of R with $R^2 = R \circ R$ and $R^3 = R \circ R \circ R$. Note that

$$R^2 = R \circ R = \{(a, a), (a, b), (a, c), (b, c), (c, c)\}$$

$$R^3 = R \circ R \circ R = \{(a, a), (a, b), (a, c), (b, c), (c, c)\}$$

Hence

$$\text{transitive}(R) = R \cup R^2 \cup R^3 = \{(a, a), (a, b), (a, c), (b, c), (c, c)\}$$

EQUIVALENCE RELATIONS AND PARTITIONS

2.18. Consider the $\mathbf{Z}$ of integers and an integer $m > 1$. We say that x is congruent to y modulo m, written

$$x \equiv y \pmod{m}$$

if $x - y$ is divisible by m. Show that this defines an equivalence relation on $\mathbf{Z}$.

We must show that the relation is reflexive, symmetric, and transitive.

(i) For any x in $\mathbf{Z}$ we have $x \equiv x \pmod{m}$ because $x - x = 0$ is divisible by m. Hence the relation is reflexive.

(ii) Suppose $x \equiv y \pmod{m}$, so $x - y$ is divisible by m. Then $-(x - y) = y - x$ is also divisible by m, so $y \equiv x \pmod{m}$. Thus the relation is symmetric.

(iii) Now suppose $x \equiv y \pmod{m}$ and $y \equiv z \pmod{m}$, so $x - y$ and $y - z$ are each divisible by m. Then the sum

$$(x - y) + (y - z) = x - z$$

is also divisible by m; hence $x \equiv z \pmod{m}$. Thus the relation is transitive.

Accordingly, the relation of congruence modulo m on $\mathbf{Z}$ is an equivalence relation.

2.19. Let A be a set of nonzero integers and let $\approx$ be the relation on $A \times A$ defined by

$$(a, b) \approx (c, d) \qquad \text{whenever} \qquad ad = bc$$

Prove that $\approx$ is an equivalence relation.

We must show that $\approx$ is reflexive, symmetric, and transitive.

(i) *Reflexivity*: We have $(a, b) \approx (a, b)$ since $ab = ba$. Hence $\approx$ is reflexive.

(ii) *Symmetry*: Suppose $(a,b) \approx (c,d)$. Then $ad = bc$. Accordingly, $cb = da$ and hence $(c,d) = (a,b)$. Thus, $\approx$ is symmetric.

(iii) *Transitivity*: Suppose $(a,b) \approx (c,d)$ and $(c,d) \approx (e,f)$. Then $ad = bc$ and $cf = de$. Multiplying corresponding terms of the equations gives $(ad)(cf) = (bc)(de)$. Canceling $c \neq 0$ and $d \neq 0$ from both sides of the equation yields $af = be$, and hence $(a,b) \approx (e,f)$. Thus $\approx$ is transitive. Accordingly, $\approx$ is an equivalence relation.

2.20. Let R be the following equivalence relation on the set $A = \{1,2,3,4,5,6\}$:

$$R = \{(1,1),(1,5),(2,2),(2,3),(2,6),(3,2),(3,3),(3,6),(4,4),(5,1),(5,5),(6,2),(6,3),(6,6)\}$$

Find the partition of A *induced by* R, i.e., find the equivalence classes of R.

Those elements related to 1 are 1 and 5 hence

$$[1] = \{1,5\}$$

We pick an element which does not belong to [1], say 2. Those elements related to 2 are 2, 3 and 6, hence

$$[2] = \{2,3,6\}$$

The only element which does not belong to [1] or [2] is 4. The only element related to 4 is 4. Thus

$$[4] = \{4\}$$

Accordingly,

$$[\{1,5\},\{2,3,6\},\{4\}]$$

is the partition of A induced by R.

2.21. Prove Theorem 2.6: Let R be an equivalence relation in a set A. Then the quotient set A/R is a partition of A. Specifically,

(i) $a \in [a]$, for every $a \in A$.

(ii) $[a] = [b]$ if and only if $(a,b) \in R$.

(iii) If $[a] \neq [b]$, then $[a]$ and $[b]$ are disjoint.

Proof of (i): Since R is reflexive, $(a,a) \in R$ for every $a \in A$ and therefore $a \in [a]$.

Proof of (ii): Suppose $(a,b) \in R$. We want to show that $[a] = [b]$. Let $x \in [b]$; then $(b,x) \in R$. But by hypothesis $(a,b) \in R$ and so, by transitivity, $(a,x) \in R$. Accordingly $x \in [a]$. Thus $[b] \subseteq [a]$. To prove that $[a] \subseteq [b]$, we observe that $(a,b) \in R$ implies, by symmetry, that $(b,a) \in R$. Then, by a similar argument, we obtain $[a] \subseteq [b]$. Consequently, $[a] = [b]$.

On the other hand, if $[a] = [b]$, then, by (i), $b \in [b] = [a]$; hence $(a,b) \in R$.

Proof of (iii): We prove the equivalent contrapositive statement:

$$\text{If } [a] \cap [b] \neq \varnothing \qquad \text{then} \qquad [a] = [b]$$

If $[a] \cap [b] \neq \varnothing$, then there exists an element $x \in A$ with $x \in [a] \cap [b]$. Hence $(a,x) \in R$ and $(b,x) \in R$. By symmetry, $(x,b) \in R$ and by transitivity, $(a,b) \in R$. Consequently by (ii), $[a] = [b]$.

2.22. Consider the set of words $W = \{\text{sheet, last, sky, wash, wind, sit}\}$. Find W/R where R is the equivalence relation on W defined by either (*a*) "has the same number of letters as"; (*b*) "begins with the same letter as".

(*a*) Those words with the same number of letters belong to the same cell; hence

$$W/R = [\{\text{sheet}\}, \{\text{last, wash, wind}\}, \{\text{sky, sit}\}].$$

(*b*) Those words beginning with the same letter belong to the same cell; hence

$$W/R = [\{\text{sheet, sky, sit}\}, \{\text{last}\}, \{\text{wash, wind}\}].$$

PARTIAL ORDERING

2.23. Let ℓ be any collection of sets. Is the relation of set inclusion $\subseteq$ a partial order on ℓ?

Yes, since set inclusion is reflexive, antisymmetric, and transitive. That is, for any sets A, B, C in ℓ we have: (i) $A \subseteq A$; (ii) if $A \subseteq B$ and $B \subseteq A$, then $A = B$; (iii) if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

2.24. Consider the set $\mathbf{Z}$ of integers. Define $a\,R\,b$ by $b = a^r$ for some positive integer r. Show that R is a partial order on $\mathbf{Z}$, that is, show that R is: (a) reflexive; (b) antisymmetric, (c) transitive.

(a) R is reflexive since $a = a^1$.

(b) Suppose $a\,R\,b$ and $b\,R\,a$, say $b = a^r$ and $a = b^s$. Then $a = (a^r)^s = a^{rs}$. There are three possibilities: (i) $rs = 1$, (ii) $a = 1$, and (iii) $a = -1$. If $rs = 1$ then $r = 1$ and $s = 1$ and so $a = b$. If $a = 1$ then $b = 1^r = 1 = a$, and, similarly, if $b = 1$ then $a = 1$. Lastly, if $a = -1$ then $b = -1$ (since $b \neq 1$) and $a = b$. In all three cases, $a = b$. Thus R is antisymmetric.

(c) Suppose $a\,R\,b$ and $b\,R\,c$ are, say, $b = a^r$ and $c = b^s$. Then $c = (a^r)^s = a^{rs}$ and, therefore, $a\,R\,c$. Hence R is transitive.

Accordingly, R is a partial order on $\mathbf{Z}$.

Supplementary Problems

RELATIONS

2.25. Let $W = \{\text{Marc, Erik, Paul}\}$ and let $V = (\text{Erik, David})$. Find: (a) $W \times V$; (b) $V \times W$; (c) $V \times V$.

2.26. Let $S = \{a, b, c\}$, $T = \{b, c, d\}$, and $W = \{a, d\}$. Construct the tree diagram of $S \times T \times W$ and then find $S \times T \times W$.

2.27. Find x and y if: (a) $(x + 2, 4) = (5, 2x + y)$; (b) $(y - 2, 2x + 1) = (x - 1, y + 2)$.

2.28. Prove: (a) $A \times (B \cap C) = (A \times B) \cap (A \times C)$; ($b$) $A \times (B \cup C) = (A \times B) \cup (A \times B)$.

2.29. Let R be the following relation on $A = \{1, 2, 3, 4\}$:

$$R = \{(1, 3), (1, 4), (3, 2), (3, 3), (3, 4)\}$$

(a) Find the matrix M_R of R.
(b) Find the domain and range of R.
(c) Find R^{-1}.
(d) Draw the directed graph of R.
(e) Find the composition relation $R \circ R$.

2.30. Let R and S be the following relations on $B = \{a, b, c, d\}$:

$$R = \{(a, a), (a, c), (c, b), (c, d), (d, b)\} \quad \text{and} \quad S = \{(b, a), (c, c), (c, d), (d, a)\}$$

Find the following composition relations: (a) $R \circ S$; (b) $S \circ R$; (c) $R \circ R$; (d) $S \circ S$.

2.31. Let R be the relation on the positive integers $\mathbf{N}$ defined by the equation $x + 3y = 12$; that is,

$$R = \{(x, y): x + 3y = 12\}$$

(*a*) Write R as a set of ordered pairs.

(*b*) Find: (i) domain of R, (ii) range of R, and (iii) R^{-1}.

(*c*) Find the composition relation $R \circ R$.

PROPERTIES OF RELATIONS

2.32. Each of the following defines a relation on the positive integers **N**:

(1) "x is greater than y". (3) $x + y = 10$.

(2) "xy is the square of an integer". (4) $x + 4y = 10$.

Determine which relations are (*a*) reflexive; (*b*) symmetric, (*c*) antisymmetric, (*d*) transitive.

2.33. Let R and S be relations on a set A. Assuming A has at least three elements, state whether each of the following statements is true or false. If it is false, give a counterexample on the set $A = \{1, 2, 3\}$:

(*a*) If R and S are symmetric then $R \cap S$ is symmetric.

(*b*) If R and S are symmetric then $R \cup S$ is symmetric.

(*c*) If R and S are reflexive then $R \cap S$ is reflexive.

(*d*) If R and S are reflexive then $R \cup S$ is reflexive.

(*e*) If R and S are transitive then $R \cup S$ is transitive.

(*f*) If R and S are antisymmetric then $R \cup S$ is antisymmetric.

(*g*) If R is antisymmetric, then R^{-1} is antisymmetric.

(*h*) If R is reflexive then $R \cap R^{-1}$ is not empty.

(*i*) If R is symmetric then $R \cap R^{-1}$ is not empty.

2.34. Suppose R and S are relations on a set A and R is antisymmetric. Prove that $R \cap S$ is antisymmetric.

EQUIVALENCE RELATIONS

2.35. Prove that if R is an equivalence relation on a set A, then R^{-1} is also an equivalence relation on A.

2.36. Let $S = \{1, 2, 3, \ldots, 19, 20\}$. Let R be the equivalence relation on S defined by $x \equiv y \pmod 5$, that is, $x - y$ is divisible by 5. Find the partition of S induced by R, i.e., the quotient set S/R.

2.37. Let $A = \{1, 2, 3, \ldots, 9\}$ and let $\sim$ be the relation on $A \times A$ defined by

$$(a, b) \sim (c, d) \qquad \text{if} \qquad a + d = b + c$$

(*a*) Prove that $\sim$ is an equivalence relation.

(*b*) Find $[(2, 5)]$, i.e., the equivalence class of $(2, 5)$.

Answers to Supplementary Problems

2.25. (*a*) $W \times V = \{$(Marc, Erik), (Marc, David), (Erik, Erik), (Erik, David), (Paul, Erik), (Paul, David)$\}$.

(*b*) $V \times W = \{$(Erik, Marc), (David, Marc), (Erik, Erik), (David, Erik), (Erik, Paul), (David, Paul)$\}$.

(*c*) $V \times V = \{$(Erik, Erik), (Erik, David), (David, Erik), (David, David)$\}$.

2.26. The tree diagram of $S \times T \times W$ is shown in Fig. 2-11. The set $S \times T \times W$ is equal to

$$\{(a,b,a),(a,b,d),(a,c,a),(a,c,d),(a,d,a),(a,d,d),$$
$$(b,b,a),(b,b,d),(b,c,a),(b,c,d),(b,d,a),(b,d,d),$$
$$(c,b,a),(c,b,d),(c,c,a),(c,c,d),(c,d,a),(c,d,d)\}$$

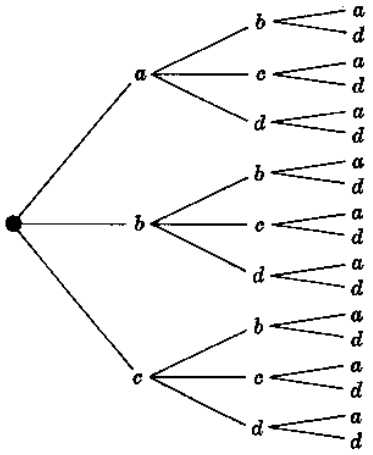


Fig. 2-11

2.27. (*a*) $x = 3;\ y = -2$; (*b*) $x = 2,\ y = 3$.

2.29. (*a*) $M_R = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$.

(*b*) Domain $= \{1,3\}$, range $= \{2,3,4\}$.
(*c*) $R^{-1} = \{(3,1),(4,1),(2,3),(3,3),(4,3)\}$.
(*d*) See Fig. 2-12.
(*e*) $R \circ R = \{(1,2),(1,3),(1,4),(3,2),(3,3),(3,4)\}$.

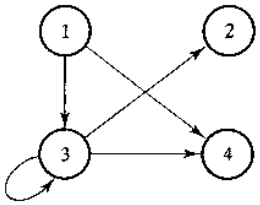


Fig. 2-12

2.30. (*a*) $R \circ S = \{(a,c),(a,d),(c,a),(d,a)\}$.
(*b*) $S \circ R = \{(b,a),(b,c),(c,b),(c,d),(d,a),(d,c)\}$.
(*c*) $R \circ R = \{(a,a),(a,b),(a,c),(a,d),(c,b)\}$.
(*d*) $S \circ S = \{(c,c),(c,a),(c,d)\}$.

2.31. (*a*) $\{(9,1),(6,2),(3,3)\}$
(*b*) (i) $\{9,6,3\}$, (ii) $\{1,2,3\}$, (iii) $\{(1,9),(2,6),(3,3)\}$
(*c*) $\{(3,3)\}$

2.32. (*a*) None; (*b*) (2) and (3); (*c*) (1) and (4); (*d*) all except (3).

2.33. All are true except (*e*) $R = \{1,2)\}$, $S = \{(2,3)\}$ and (*f*) $R = \{(1,2)\}$, $S = \{(2,1)\}$.

2.36. $[\{1,6,11,16\}, \{2,7,12,17\}, \{3,8,13,18\}, \{4,9,14,19\}, \{5,10,15,20\}]$

2.37. (*b*) $\{(1,4),(2,5),(3,6),(4,7),(5,8),(6,9)\}$

© The McGraw–Hill Companies, 2004

Chapter 3

Functions and Algorithms

3.1 INTRODUCTION

One of the most important concepts in mathematics is that of a function. The terms "map", "mapping", "transformation", and many others mean the same thing; the choice of which word to use in a given situation is usually determined by tradition and the mathematical background of the person using the term.

Related to the notion of a function is that of an algorithm. The notation for presenting an algorithm and a discussion of its complexity is also covered in this chapter.

3.2 FUNCTIONS

Suppose that to each element of a set A we assign a unique element of a set B; the collection of such assignments is called a *function* from A into B. The set A is called the *domain* of the function, and the set B is called the *codomain*.

Functions are ordinarily denoted by symbols. For example, let f denote a function from A into B. Then we write

$$f: A \to B$$

which is read: "f is a function from A into B", or "f takes (or; maps) A into B". If $a \in A$, then $f(a)$ (read: "f of a") denotes the unique element of B which f assigns to a; it is called the *image* of a under f, or the *value* of f at a. The set of all image values is called the *range* or *image* of f. The image of $f: A \to B$ is denoted by Ran (f), Im (f) or $f(A)$.

Frequently, a function can be expressed by means of a mathematical formula. For example, consider the function which sends each real number into its square. We may describe this function by writing

$$f(x) = x^2 \qquad \text{or} \qquad x \mapsto x^2 \qquad \text{or} \qquad y = x^2$$

In the first notation, x is called a *variable* and the letter f denotes the function. In the second notation, the barred arrow $\mapsto$ is read "goes into". In the last notation, x is called the *independent variable* and y is called the *dependent variable* since the value of y will depend on the value of x.

Remark: Whenever a function is given by a formula in terms of a variable x, we assume, unless it is otherwise stated, that the domain of the function is **R** (or the largest subset of **R** for which the formula has meaning) and the codomain is **R**.

EXAMPLE 3.1

(*a*) Consider the function $f(x) = x^3$, i.e., f assigns to each real number its cube. Then the image of 2 is 8, and so we may write $f(2) = 8$.

(*b*) Let f assign to each country in the world its capital city. Here the domain of f is the set of countries in the world; the codomain is the list of cities of the world. The image of France is Paris; or, in other words, $f(\text{France}) = \text{Paris}$.

(*c*) Figure 3-1 defines a function f from $A = \{a, b, c, d\}$ into $B = \{r, s, t, u\}$ in the obvious way. Here

$$f(a) = s, \qquad f(b) = u, \qquad f(c) = r, \qquad f(d) = s$$

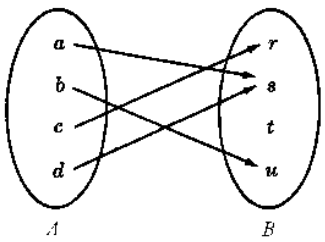


Fig. 3-1

The image of f is the set of image values, $\{r, s, u\}$. Note that t does not belong to the image of f because t is not the image of any element under f.

(*d*) Let A be any set. The function from A into A which assigns to each element that element itself is called the *identity function* on A and is usually denoted by 1_A or simply 1. In other words,

$$1_A(a) = a$$

for every element a in A.

(*e*) Suppose S is a subset of A, that is, suppose $S \subseteq A$. The *inclusion map* or *embedding* of S into A, denoted by i: $S \hookrightarrow A$, is the function defined by

$$i(x) = x$$

for every $x \in S$; and the *restriction* to S of any function f: $A \to B$, denoted by $f|_S$, is the function from S to B defined by

$$f|_A(x) = f(x)$$

for every $x \in S$.

Functions as Relations

There is another point of view from which functions may be considered. First of all, every function f: $A \to B$ gives rise to a relation from A to B called the *graph of* f and defined by

$$\text{Graph of } f = \{(a, b)\colon a \in A, b = f(a)\}$$

Two functions f: $A \to B$ and g: $A \to B$ are defined to be equal, written $f = g$, if $f(a) = g(a)$ for every $a \in A$; that is, if they have the same graph. Accordingly, we do not distinguish between a function and its graph. Now, such a graph relation has the property that each a in A belongs to a unique ordered pair (a, b) in the relation. On the other hand, any relation f from A to B that has this property gives rise to a function f: $A \to B$, where $f(a) = b$ for each (a, b) in f. Consequently, one may equivalently define a function as follows:

Definition: A function f: $A \to B$ is a relation from A to B (i.e., a subset of $A \times B$) such that each $a \in A$ belongs to a unique ordered pair (a, b) in f.

Although we do not distinguish between a function and its graph, we will still use the terminology "graph of f" when referring to f as a set of ordered pairs. Moreover, since the graph of f is a relation, we can draw its picture as was done for relations in general, and this pictorial representation is itself sometimes called the graph of f. Also, the defining condition of a function, that each $a \in A$ belongs to a unique pair (a, b) in f, is equivalent to the geometrical condition of each vertical line intersecting the graph in exactly one point.

EXAMPLE 3.2

(*a*) Let f: $A \to B$ be the function defined in Example 3.1(*c*). Then the graph of f is the following set of ordered pairs:

$$\{(a, s), (b, u), (c, r), (d, s)\}$$

(*b*) Consider the following relations on the set $A = \{1, 2, 3\}$:

$$f = \{(1, 3), (2, 3), (3, 1)$$
$$g = \{(1, 2), (3, 1)\}$$
$$h = \{(1, 3), (2, 1), (1, 2), (3, 1)\}$$

f is a function from A into A since each member of A appears as the first coordinate in exactly one ordered pair in f; here $f(1) = 3$, $f(2) = 3$ and $f(3) = 1$. g is not a function from A into A since $2 \in A$ is not the first coordinate of any pair in g and so g does not assign any image to 2. Also h is not a function from A into A

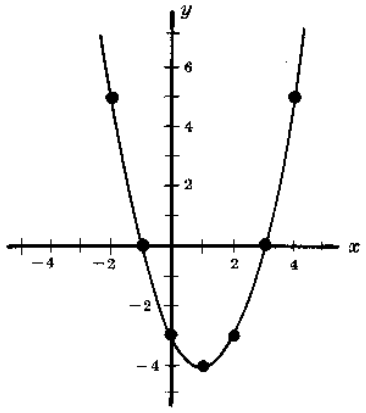
since $1 \in A$ appears as the first coordinate of two distinct ordered pairs in h, $(1,3)$ and $(1,2)$. If h is to be a function it cannot assign both 3 and 2 to the element $1 \in A$.

(*c*) By a real polynomial function, we mean a function f: $\mathbf{R} \to \mathbf{R}$ of the form

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

where the a_i are real numbers. Since $\mathbf{R}$ is an infinite set, it would be impossible to plot each point of the graph. However, the graph of such a function can be approximated by first plotting some of its points and then drawing a smooth curve through these points. The points are usually obtained from a table where various values are assigned to x and the corresponding values of $f(x)$ are computed. Figure 3-2 illustrates this technique using the function $f(x) = x^2 - 2x - 3$.

x	$f(x)$
−2	5
−1	0
0	−3
1	−4
2	−3
3	0
4	5



Graph of $f(x) = x^2 - 2x - 3$

Fig. 3-2

Composition Function

Consider functions f: $A \to B$ and g: $B \to C$; that is, where the codomain of f is the domain of g. Then we may define a new function from A to C, called the *composition* of f and g and written $g \circ f$, as follows:

$$(g \circ f)(a) \equiv g(f(a))$$

That is, we find the image of a under f and then find the image of $f(a)$ under g. This definition is not really new. If we view f and g as relations, then this function is the same as the composition of f and g as relations (see Section 2.6) except that here we use the functional notation $g \circ f$ for the composition of f and g instead of the notation $f \circ g$ which was used for relations.

Consider any function f: $A \to B$. Then

$$f \circ 1_A = f \qquad \text{and} \qquad 1_B \circ f = f$$

where 1_A and 1_B are the identity functions on A and B, respectively.

3.3 ONE-TO-ONE, ONTO, AND INVERTIBLE FUNCTIONS

A function f: $A \to B$ is said to be *one-to-one* (written 1-1) if different elements in the domain A have distinct images. Another way of saying the same thing is that f is *one-to-one* if $f(a) = f(a')$ implies $a = a'$.

A function $f: A \to B$ is said to be an *onto* function if each element of B is the image of some element of A. In other words, $f: A \to B$ is onto if the image of f is the entire codomain, i.e., if $f(A) = B$. In such a case we say that f is a function from A *onto* B or that f maps A *onto* B.

A function $f: A \to B$ is *invertible* if its inverse relation f^{-1} is a function from B to A. In general, the inverse relation f^{-1} may not be a function. The following theorem gives simple criteria which tells us when it is.

Theorem 3.1: A function $f: A \to B$ is invertible if and only if f is both one-to-one and onto.

If $f: A \to B$ is one-to-one and onto, then f is called a *one-to-one correspondence* between A and B. This terminology comes from the fact that each element of A will then correspond to a unique element of B and vice versa.

Some texts use the terms *injective* for a one-to-one function, *surjective* for an onto function, and *bijective* for a one-to-one correspondence.

EXAMPLE 3.3 Consider the functions $f_1: A \to B$, $f_2: B \to C$, $f_3: C \to D$ and $f_4: D \to E$ defined by the diagram of Fig. 3-3. Now f_1 is one-to-one since no element of B is the image of more than one element of A. Similarly, f_2 is one-to-one. However, neither f_3 nor f_4 is one-to-one since $f_3(r) = f_3(u)$ and $f_4(v) = f_4(w)$.

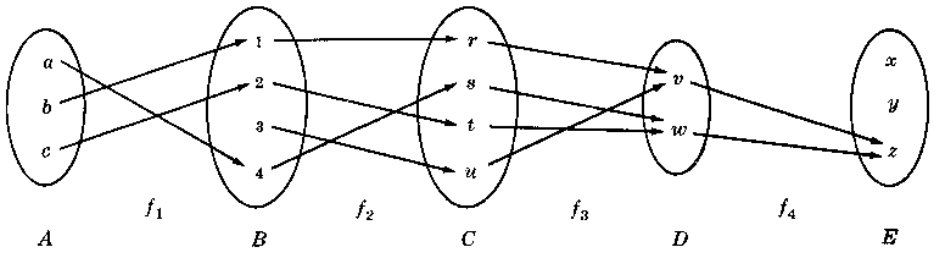


Fig. 3-3

As far as being onto is concerned, f_2 and f_3 are both onto functions since every element of C is the image under f_2 of some element of B and every element of D is the image under f_3 of some element of C, i.e., $f_2(B) = C$ and $f_3(C) = D$. On the other hand, f_1 is not onto since $3 \in B$ is not the image under f_1 of any element of A, and f_4 is not onto since $x \in E$ is not the image under f_4 of any element of D.

Thus f_1 is one-to-one but not onto, f_3 is onto but not one-to-one and f_4 is neither one-to-one nor onto. However, f_2 is both one-to-one and onto, i.e., is a one-to-one correspondence between A and B. Hence f_2 is invertible and f_2^{-1} is a function from C to B.

Geometrical Characterization of One-to-One and Onto Functions

Since functions may be identified with their graphs, and since graphs may be plotted, we might wonder whether the concepts of being one-to-one and onto have geometrical meaning. We show that the answer is yes.

To say that a function $f: A \to B$ is one-to-one means that there are no two distinct pairs (a_1, b) and (a_2, b) in the graph of f; hence each horizontal line can intersect the graph of f in at most one point. On the other hand, to say that f is an onto function means that for every $b \in B$ there must be at least one $a \in A$ such that (a, b) belongs to the graph of f; hence each horizontal line must intersect the graph of f at least once. Accordingly, if f is both one-to-one and onto, i.e. invertible, then each horizontal line will intersect the graph of f in exactly one point.

EXAMPLE 3.4 Consider the following four functions from **R** into **R**:

$$f_1(x) = x^2, \qquad f_2(x) = 2^x, \qquad f_3(x) = x^3 - 2x^2 - 5x + 6, \qquad f_4(x) = x^3$$

The graphs of these functions appear in Fig. 3-4. Observe that there are horizontal lines which intersect the graph of f_1 twice and there are horizontal lines which do not intersect the graph of f_1 at all; hence f_1 is neither one-to-one nor onto. Similarly, f_2 is one-to-one but not onto, f_3 is onto but not one-to-one and f_4 is both one-to-one and onto. The inverse of f_4 is the cube root function, i.e., $f_4^{-1}(x) = \sqrt[3]{x}$.

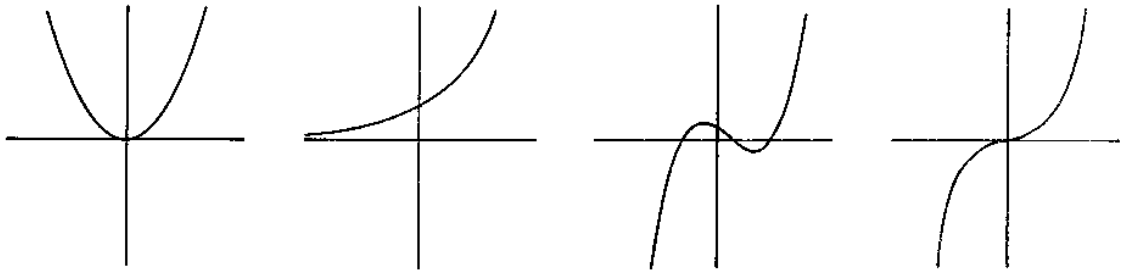


Fig. 3-4

3.4 MATHEMATICAL FUNCTIONS, EXPONENTIAL AND LOGARITHMIC FUNCTIONS

This section presents various mathematical functions which appear often in the analysis of algorithms, and in computer science in general, together with their notation. We also discuss the exponential and logarithmic functions, and their relationship.

Floor and Ceiling Functions

Let x be any real number. Then x lies between two integers called the floor and the ceiling of x. Specifically,

$\lfloor x \rfloor$, called the *floor* of x, denotes the greatest integer that does not exceed x.
$\lceil x \rceil$, called the *ceiling* of x, denotes the least integer that is not less than x.

If x is itself an integer, then $\lfloor x \rfloor = \lceil x \rceil$; otherwise $\lfloor x \rfloor + 1 = \lceil x \rceil$. For example,

$$\lfloor 3.14 \rfloor = 3, \quad \lfloor \sqrt{5} \rfloor = 2, \quad \lfloor -8.5 \rfloor = -9, \quad \lfloor 7 \rfloor = 7, \quad \lfloor -4 \rfloor = -4$$
$$\lceil 3.14 \rceil = 4, \quad \lceil \sqrt{5} \rceil = 3, \quad \lceil -8.5 \rceil = -8, \quad \lceil 7 \rceil = 7, \quad \lceil -4 \rceil = -4$$

Integer and Absolute Value Functions

Let x be any real number. The *integer value* of x, written $\text{INT}(x)$, converts x into an integer by deleting (truncating) the fractional part of the number. Thus

$$\text{INT}(3.14) = 3, \qquad \text{INT}(\sqrt{5}) = 2, \qquad \text{INT}(-8.5) = -8, \qquad \text{INT}(7) = 7$$

Observe that $\text{INT}(x) = \lfloor x \rfloor$ or $\text{INT}(x) = \lceil x \rceil$ according to whether x is positive or negative.

The *absolute value* of the real number x, written $\text{ABS}(x)$ or $|x|$, is defined as the greater of x or $-x$. Hence $\text{ABS}(0) = 0$, and, for $x \neq 0$, $\text{ABS}(x) = x$ or $\text{ABS}(x) = -x$, depending on whether x is positive or negative. Thus

$$|-15| = 15, \qquad |7| = 7, \qquad |-3.33| = 3.33, \qquad |4.44| = 4.44, \qquad |-0.075| = 0.075$$

We note that $|x| = |-x|$ and, for $x \neq 0$, $|x|$ is positive.

Remainder Function; Modular Arithmetic

Let k be any integer and let M be a positive integer. Then

$$k \pmod{M}$$

(read *k modulo M*) will denote the integer remainder when k is divided by M. More exactly, $k \pmod{M}$ is the unique integer r such that

$$k = Mq + r \qquad \text{where} \qquad 0 \le r < M$$

When k is positive, simply divide k by M to obtain the remainder r. Thus

$$25 \pmod 7 = 4, \qquad 25 \pmod 5 = 0, \qquad 35 \pmod{11} = 2, \qquad 3 \pmod 8 = 3$$

If k is negative, divide $|k|$ by M to obtain a remainder r'; then $k \pmod M = M - r'$ when $r' \neq 0$. Thus

$$-26 \pmod 7 = 7 - 5 = 2, \qquad -371 \pmod 8 = 8 - 3 = 5, \qquad -39 \pmod 3 = 0$$

The term "mod" is also used for the mathematical congruence relation, which is denoted and defined as follows:

$$a \equiv b \pmod{M} \qquad \text{if and only if} \qquad M \text{ divides } b - a$$

M is called the *modulus*, and $a \equiv b \pmod M$ is read "a is congruent to b modulo M". The following aspects of the congruence relation are frequently useful:

$$0 \equiv M \pmod{M} \qquad \text{and} \qquad a \pm M \equiv a \pmod{M}$$

Arithmetic modulo M refers to the arithmetic operations of addition, multiplication, and subtraction where the arithmetic value is replaced by its equivalent value in the set

$$\{0, 1, 2, \ldots, M - 1\}$$

or in the set

$$\{1, 2, 3, \ldots, M\}$$

For example, in arithmetic modulo 12, sometimes called "clock" arithmetic,

$$6 + 9 \equiv 3, \qquad 7 \times 5 \equiv 11, \qquad 1 - 5 \equiv 8, \qquad 2 + 10 \equiv 0 \equiv 12$$

(The use of 0 or M depends on the application.)

Exponential Functions

Recall the following definitions for integer exponents (where m is a positive integer):

$$a^m = a \cdot a \cdots a \,(m \text{ times}), \qquad a^0 = 1, \qquad a^{-m} = \frac{1}{a^m}$$

Exponents are extended to include all rational numbers by defining, for any rational number m/n,

$$a^{m/n} = \sqrt[n]{a^m} = (\sqrt[n]{a})^m$$

For example,

$$2^4 = 16, \qquad 2^{-4} = \frac{1}{2^4} = \frac{1}{16}, \qquad 125^{2/3} = 5^2 = 25$$

In fact, exponents are extended to include all real numbers by defining, for any real number x,

$$a^x = \lim_{r \to x} a^r, \qquad \text{where } r \text{ is a rational number}$$

Accordingly, the exponential function $f(x) = a^x$ is defined for all real numbers.

Logarithmic Functions

Logarithms are related to exponents as follows. Let b be a positive number. The logarithm of any positive number x to be the base b, written

$$\log_b x$$

represents the exponent to which b must be raised to obtain x. That is,

$$y = \log_b x \qquad \text{and} \qquad b^y = x$$

are equivalent statements. Accordingly,

$$\log_2 8 = 3 \quad \text{since} \quad 2^3 = 8; \qquad \log_{10} 100 = 2 \quad \text{since} \quad 10^2 = 100$$
$$\log_2 64 = 6 \quad \text{since} \quad 2^6 = 64; \qquad \log_{10} 0.001 = -3 \quad \text{since} \quad 10^{-3} = 0.001$$

Furthermore, for any base b,

$$\log_b 1 = 0 \quad \text{since} \quad b^0 = 1$$
$$\log_b b = 1 \quad \text{since} \quad b^1 = b$$

The logarithm of a negative number and the logarithm of 0 are not defined.

Frequently, logarithms are expressed using approximate values. For example, using tables or calculators, one obtains

$$\log_{10} 300 = 2.4771 \qquad \text{and} \qquad \log_e 40 = 3.6889$$

as approximate answers. (Here $e = 2.718281\ldots$.)

Three classes of logarithms are of special importance: logarithms to base 10, called *common logarithms*; logarithms to base e, called *natural logarithms*; and logarithms to base 2, called *binary logarithms*. Some texts write

$$\ln x \quad \text{for} \quad \log_e x \qquad \text{and} \qquad \lg x \quad \text{or} \quad \text{Log } x \quad \text{for} \quad \log_2 x$$

The term log x, by itself, usually means $\log_{10} x$; but it is also used for $\log_e x$ in advanced mathematical texts and for $\log_2 x$ in computer science texts.

Frequently, we will require only the floor or the ceiling of a binary logarithm. This can be obtained by looking at the powers of 2. For example,

$$\lfloor \log_2 100 \rfloor = 6 \quad \text{since} \quad 2^6 = 64 \quad \text{and} \quad 2^7 = 128$$
$$\lceil \log_2 1000 \rceil = 9 \quad \text{since} \quad 2^8 = 512 \quad \text{and} \quad 2^9 = 1024$$

and so on.

Relationship between the Exponential and Logarithmic Functions

The basic relationship between the exponential and the logarithmic functions

$$f(x) = b^x \qquad \text{and} \qquad g(x) = \log_b x$$

is that they are inverses of each other; hence the graphs of these functions are related geometrically. This relationship is illustrated in Fig. 3-5 where the graphs of the exponential function $f(x) = 2^x$, the logarithmic function $g(x) = \log_2 x$, and the linear function $h(x) = x$ appear on the same coordinate axis. Since $f(x) = 2^x$ and $g(x) = \log_2 x$ are inverse functions, they are symmetric with respect to the linear function $h(x) = x$ or, in other words, the line $y = x$.

Figure 3-5 also indicates another important property of the exponential and logarithmic functions. Specifically, for any positive c, we have

$$g(c) < h(c) < f(c)$$

In fact, as c increases in value, the vertical distances $h(c) - g(c)$ and $f(c) - g(c)$ increase in value. Moreover, the logarithmic function $g(x)$ grows very slowly compared with the linear function $h(x)$, and the exponential function $f(x)$ grows very quickly compared with $h(x)$.

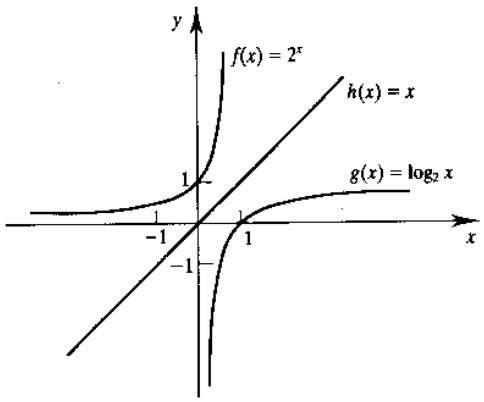


Fig. 3-5

3.5 SEQUENCES, INDEXED CLASSES OF SETS

Sequences and indexed classes of sets are special types of functions with their own notation. We discuss these objects in this section. We also discuss the summation notation here.

Sequences

A *sequence* is a function from the set $\mathbf{N} = \{1, 2, 3, \ldots\}$ of positive integers into a set A. The notation a_n is used to denote the image of the integer n. Thus a sequence is usually denoted by

$$a_1, a_2, a_3, \ldots \qquad \text{or} \qquad \{a_n : n \in \mathbf{N}\} \qquad \text{or simply} \qquad \{a_n\}$$

Sometimes the domain of a sequence is the set $\{0, 1, 2, \ldots\}$ of nonnegative integers rather than $\mathbf{N}$. In such a case we say n begins with 0 rather than 1.

A *finite sequence* over a set A is a function from $\{1, 2, \ldots, m\}$ into A, and it is usually denoted by

$$a_1, a_2, \ldots, a_m$$

Such a finite sequence is sometimes called a *list* or an *m-tuple*.

EXAMPLE 3.5

(*a*) The familiar sequences

$$1, \tfrac{1}{2}, \tfrac{1}{3}, \tfrac{1}{4}, \ldots \qquad \text{and} \qquad 1, \tfrac{1}{2}, \tfrac{1}{4}, \tfrac{1}{8}, \ldots$$

may be formally defined, respectively, by

$$a_n = 1/n \qquad \text{and} \qquad b_n = 2^{-n}$$

where the first sequence begins with $n = 1$ and the second sequence begins with $n = 0$.

(*b*) The important sequence 1, −1, 1, −1, ... may be formally defined by

$$a_n = (-1)^{n+1} \qquad \text{or, equivalently, by} \qquad b_n = (-1)^n$$

where the first sequence begins with $n = 1$ and the second sequence begins with $n = 0$.

(*c*) (***Strings***) Suppose a set A is finite and A is viewed as a character set or an alphabet. Then a finite sequence over A is called a *string* or *word*, and it is usually written in the form $a_1a_2 \dots a_m$, that is, without parenthesis. The number m of characters in the string is called its *length*. One also views the set with zero characters as a string; it is called the *empty string* or *null string*. Strings over an alphabet A and certain operations on these strings will be discussed in detail in Chapter 13.

Summation Symbol, Sums

Here we introduce the summation symbol $\sum$ (the Greek letter sigma). Consider a sequence $a_1, a_2, a_3, \dots$. Then the sums

$$a_1 + a_2 + \cdots + a_n \qquad \text{and} \qquad a_m + a_{m+1} + \cdots + a_n$$

will be denoted, respectively, by

$$\sum_{j=1}^{n} a_j \qquad \text{and} \qquad \sum_{j=m}^{n} a_j$$

The letter j in the above expressions is called a *dummy index* or *dummy variable*. Other letters frequently used as dummy variables are i, k, s and t.

EXAMPLE 3.6

$$\sum_{i=1}^{n} a_i b_i = a_1 b_1 + a_2 b_2 + \ldots + a_n b_n$$

$$\sum_{j=2}^{5} j^2 = 2^2 + 3^2 + 4^2 + 5^2 = 4 + 9 + 16 + 25 = 54$$

$$\sum_{j=1}^{n} j = 1 + 2 + \cdots + n$$

The last sum in Example 3.6 appears often. It has the value $n(n+1)/2$. That is,

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$$

Thus, for example,

$$1 + 2 + \cdots + 50 = \frac{50(51)}{2} = 1275$$

Indexed Classes of Sets

Let I be any nonempty set, and let S be a collection of sets. An *indexing function* from I to S is a function $f\colon I \to S$. For any $i \in I$, we denote the image $f(i)$ by A_i. Thus the indexing function f is usually denoted by

$$\{A_i\colon i \in I\} \qquad \text{or} \qquad \{A_i\}_{i \in I} \qquad \text{or simply} \qquad \{A_i\}$$

The set I is called the *indexing set*, and the elements of I are called *indices*. If f is one-to-one and onto, we say that S is indexed by I.

The concepts of union and intersection are defined for indexed classes of sets by

$$\cup_{i \in I} A_i = \{x\colon x \in A_i \text{ for some } i \in I\} \qquad \text{and} \qquad \cap_{i \in I} A_i = \{x\colon x \in A_i \text{ for all } i \in I\}$$

In the case that I is a finite set, this is just the same as our previous definitions of union and intersection. If I is $\mathbf{N}$, we may denote the union and intersection by

$$A_1 \cup A_2 \cup \cdots \qquad \text{and} \qquad A_1 \cap A_2 \cap \cdots$$

respectively.

EXAMPLE 3.7 Let I be the set $\mathbf{Z}$ of integers. To each integer n we assign the following subset of $\mathbf{R}$:

$$A_n = \{x\colon x \le n\}$$

In other words, A_n is the infinite interval $(-\infty, n]$.) For any real number a, there exist integers n_1 and n_2 such that $n_1 < a < n_2$; so $a \in A_{n_2}$ but $a \notin A_{n_1}$. Hence

$$a \in \cup_n A_n \qquad \text{but} \qquad a \notin \cap_n A_n$$

Accordingly,

$$\cup_n A_n = \mathbf{R} \qquad \text{but} \qquad \cap_n A_n = \varnothing$$

3.6 RECURSIVELY DEFINED FUNCTIONS

A function is said to be *recursively defined* if the function definition refers to itself. In order for the definition not to be circular, the function definition must have the following two properties:

(1) There must be certain arguments, called *base values*, for which the function does not refer to itself.
(2) Each time the function does refer to itself, the argument of the function must be closer to a base value.

A recursive function with these two properties is said to be *well-defined*.

The following examples should help clarify these ideas.

Factorial Function

The product of the positive integers from 1 to n, inclusive, is called "n factorial" and is usually denoted by $n!$; that is,

$$n! = 1 \cdot 2 \cdot 3 \cdots (n-2)(n-1)n$$

It is also convenient to define $0! = 1$, so that the function is defined for all nonnegative integers. Thus we have

$$0! = 1, \qquad 1! = 1, \qquad 2! = 1 \cdot 2 = 2, \qquad 3! = 1 \cdot 2 \cdot 3 = 6, \qquad 4! - 1 \cdot 2 \cdot 3 \cdot 4 = 24,$$

$$5! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 = 120, \qquad 6! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 = 720$$

and so on. Observe that

$$5! = 5 \cdot 4! = 5 \cdot 24 = 120 \qquad \text{and} \qquad 6! = 6 \cdot 5! = 6 \cdot 120 = 720$$

This is true for every positive integer n; that is,

$$n! = n \cdot (n-1)!$$

Accordingly, the factorial function may also be defined as follows:

Definition 3.1 (**Factorial Function**):

(*a*) If $n = 0$, then $n! = 1$.
(*b*) If $n > 0$, then $n! = n \cdot (n-1)!$

Observe that the above definition of n! is recursive, since it refers to itself when it uses $(n-1)!$. However:

(1) The value of $n!$ is explicitly given when $n = 0$ (thus 0 is a base value).
(2) The value of $n!$ for arbitrary n is defined in terms of a smaller value of n which is closer to the base value 0.

Accordingly, the definition is not circular, or, in other words, the function is well-defined.

EXAMPLE 3.8 Let us calculate 4! using the recursive definitions. This calculation requires the following nine steps:

(1) $4! = 4 \cdot 3!$
(2) $3! = 3 \cdot 2!$
(3) $2! = 2 \cdot 1!$
(4) $1! = 1 \cdot 0!$
(5) $0! = 1$
(6) $1! = 1 \cdot 1 = 1$
(7) $2! = 2 \cdot 1 = 2$
(8) $3! = 3 \cdot 2 = 6$
(9) $4! = 4 \cdot 6 = 24$

That is:

Step 1. This defines 4! in terms of 3!, so we must postpone evaluating 4! until we evaluate 3! This postponement is indicated by indenting the next step.

Step 2. Here 3! is defined in terms of 2!, so we must postpone evaluating 3! until we evaluate 2!

Step 3. This defines 2! in terms of 1!

Step 4. This defines 1! in terms of 0!

Step 5. This step can explicitly evaluate 0!, since 0 is the base value of the recursive definition.

Steps 6 to 9. We backtrack, using 0! to find 1!, using 1! to find 2!, using 2! to find 3!, and finally using 3! to find 4! This backtracking is indicated by the "reverse" indention.

Observe that we backtrack in the reverse order of the original postponed evaluations.

Level Numbers

Let P be a procedure or recursive formula which is used to evaluate $f(X)$ where f is a recursive function and X is the input. We associate a *level number* with each execution of P as follows. The original execution of P is assigned level 1; and each time P is executed because of a recursive call, its level is one more than the level of the execution that made the recursive call. The *depth* of recursion in evaluating $f(X)$ refers to the maximum level number of P during its execution.

Consider, for example, the evaluation of 4! Example 3.8, which uses the recursive formula $n! = n(n-1)!$. Step 1 belongs to level 1 since it is the first execution of the formula. Thus:

Step 2 belongs to level 2; Step 3 to level 3, ...; Step 5 to level 5.

On the other hand, Step 6 belongs to level 4 since it is the result of a return from level 5. In other words, Step 6 and Step 4 belong to the same level of execution. Similarly,

Step 7 belongs to level 3; Step 8 to level 2; and Step 9 to level 1.

Accordingly, in evaluating 4!, the depth of the recursion is 5.

Fibonacci Sequence

The celebrated Fibonacci sequence (usually denoted by $F_0, F_1, F_2, \ldots$) is as follows:

$$0, \quad 1, \quad 1, \quad 2, \quad 3, \quad 5, \quad 8, \quad 13, \quad 21, \quad 34, \quad 55, \ldots$$

That is, $F_0 = 0$ and $F_1 = 1$ and each succeeding term is the sum of the two preceding terms. For example, the next two terms of the sequence are

$$34 + 55 = 89 \qquad \text{and} \qquad 55 + 89 = 144$$

A formal definition of this function follows:

Definition 3.2 (Fibonacci Sequence):

(*a*) If $n = 0$ or $n = 1$, then $F_n = n$.
(*b*) If $n > 1$, then $F_n = F_{n-2} + F_{n-1}$.

This is another example of a recursive definition, since the definition refers to itself when it uses F_{n-2} and F_{n-1}. However:

(1) The base values are 0 and 1.
(2) The value of F_n is defined in terms of smaller values of n which are closer to the base values.

Accordingly, this function is well-defined.

Ackermann Function

The Ackermann function is a function with two arguments, each of which can be assigned any nonnegative interger, that is, 0, 1, 2, ... This function is defined as follows:

Definition 3.3 (Ackermann Function):

(*a*) If $m = 0$, then $A(m, n) = n + 1$.
(*b*) If $m \neq 0$ but $n = 0$, then $A(m, n) = A(m - 1, 1)$.
(*c*) If $m \neq 0$ and $n \neq 0$, then $A(m, n) = A(m - 1, A(m, n - 1))$

Once more, we have a recursive definition, since the definition refers to itself in parts (*b*) and (*c*). Observe that $A(m, n)$ is explicitly given only when $m = 0$. The base criteria are the pairs

$$(0, 0), \quad (0, 1), \quad (0, 2), \quad (0, 3), \ldots, (0, n), \ldots$$

Although it is not obvious from the definition, the value of any $A(m, n)$ may eventually be expressed in terms of the value of the function on one or more of the base pairs.

The value of $A(1, 3)$ is calculated in Problem 3.24. Even this simple case requires 15 steps. Generally speaking, the Ackermann function is too complex to evaluate on any but a trivial example. Its importance comes from its use in mathematical logic. The function is stated here mainly to give another example of a classical recursive function and to show that the recursion part of a definition may be complicated.

3.7 CARDINALITY

Two sets A and B are said to be *equipotent*, or to have the *same number of elements* or the *same cardinality*, written $A \simeq B$, if there exists a one-to-one correspondence f: $A \to B$. A set A is *finite* if A is empty or if A has the same cardinality as the set $\{1, 2, \ldots, n\}$ for some positive integer n. A set is *infinite* if it is not finite. Familiar examples of infinite sets are the natural numbers **N**, the integers **Z**, the rational numbers **Q**, and the real numbers **R**.

We now introduce the idea of "cardinal numbers". We will consider cardinal numbers simply as symbols assigned to sets in such a way that two sets are assigned the same symbol if and only if they have the same cardinality. The cardinal number of a set A is commonly denoted by $|A|$, $n(A)$, or card (A). We will use $|A|$.

We use the obvious symbols for the cardinal numbers of finite sets. That is, 0 is assigned to the empty set $\varnothing$, and n is assigned to the set $\{1, 2, \ldots, n\}$. Thus $|A| = n$ if and only if A has the same cardinality as $\{1, 2, \ldots, n\}$, which implies that A has n elements.

The cardinal number of the infinite set **N** of positive integers is $\aleph_0$ ("aleph-naught"). This symbol was introduced by Cantor. Thus $|A| = \aleph_0$ if and only if A has the same cardinality as **N**.

EXAMPLE 3.9

(*a*) $|\{x, y, z\}| = 3$ and $|\{1, 3, 5, 7, 9\}| = 5$.

(*b*) Let $E = \{2, 4, 6, \ldots\}$, the set of even positive integers. The function $f: \mathbf{N} \to E$ defined by $f(n) = 2n$ is a one-to-one correspondence between the positive integers $\mathbf{N}$ and E. Thus E has the same cardinality as $\mathbf{N}$ and so we may write

$$|E| = \aleph_0$$

A set with cardinality $\aleph_0$ is said to be *denumerable* or *countably infinite*. A set which is finite or denumerable is said to be *countable*. One can show that the set $\mathbf{Q}$ of rational numbers is countable. In fact, we have the following theorem (proved in Problem 3.15) which we will use subsequently.

Theorem 3.2: A countable union of countable sets is countable.

In other words, if $A_1, A_2, \ldots$ are each countable sets then the union

$$A_1 \cup A_2 \cup A_3 \cup \cdots$$

is also a countable set.

An important example of an infinite set which is uncountable, i.e., not countable, is given by the following theorem which is proved in Problem 3.16.

Theorem 3.3: The set I of all real numbers between 0 and 1 is uncountable.

Inequalities and Cardinal Numbers

One also wants to compare the size of two sets. This is done by means of an inequality relation which is defined for cardinal numbers as follows. For any sets A and B, we define $|A| \leq |B|$ if there exists a function $f: A \to B$ which is one-to-one. We also write

$$|A| < |B| \quad \text{if} \quad |A| \leq |B| \quad \text{but} \quad |A| \neq |B|$$

For example, $|\mathbf{N}| < |I|$, where $I = \{x: 0 \leq x \leq 1\}$, since the function $f: \mathbf{N} \to I$ defined by $f(n) = 1/n$ is one-to-one, but $|\mathbf{N}| \neq |I|$ by Theorem 3.3.

Cantor's theorem, which follows and which we prove in Problem 3.28, tells us that the cardinal numbers are unbounded.

Theorem 3.4 (Cantor): For any set A, we have $|A| < |\text{Power}(A)|$ (where $\text{Power}(A)$ is the power set of A, i.e., the collection of all subsets of A).

The next theorem tells us that the inequality relation for cardinal numbers is antisymmetric.

Theorem 3.5 (Schroeder-Bernstein): Suppose A and B are sets such that

$$|A| \leq |B| \quad \text{and} \quad |B| \leq |A|$$

Then $|A| = |B|$.

We prove an equivalent formulation of this theorem in Problem 3.29.

3.8 ALGORITHMS AND FUNCTIONS

An algorithm M is a finite step-by-step list of well-defined instructions for solving a particular problem, say, to find the output $f(X)$ for a given function f with input X. (Here X may be a list or set of values.) Frequently, there may be more than one way to obtain $f(X)$, as illustrated by the following examples. The particular choice of the algorithm M to obtain $f(X)$ may depend on the "efficiency" or "complexity" of the algorithm; this question of the complexity of an algorithm M is formally discussed in the next section.

EXAMPLE 3.10 (Polynomial Evaluation) Suppose, for a given polynomial $f(x)$ and value $x = a$, we want to find $f(a)$, say,

$$f(x) = 2x^3 - 7x^2 + 4x - 15 \qquad \text{and} \qquad a = 5$$

This can be done in the following two ways.

(*a*) (***Direct Method***): Here we substitute $a = 5$ directly in the polynomial to obtain

$$f(5) = 2(125) - 7(25) + 4(5) - 7 = 250 - 175 + 20 - 15 = 80$$

Observe that there are $3 + 2 + 1 = 6$ multiplications and 3 additions. In general, evaluating a polynomial of degree n directly would require approximately.

$$n + (n-1) + \cdots + 1 = \frac{n(n+1)}{2} \text{ multiplications} \qquad \text{and} \qquad n \text{ additions}$$

(*b*) (***Horner's Method or Synthetic Division***): Here we rewrite the polynomial by successively factoring out x (on the right) as follows:

$$f(x) = (2x^2 - 7x + 4)x - 15 = (((2x - 7)x + 4)x - 15$$

Then

$$f(5) = ((3)5 + 4)5 - 15 = (19)5 - 15 = 95 - 15 = 80$$

For those familiar with synthetic division, the above arithmetic is equivalent to the following synthetic division:

$$\begin{array}{r|cccccccc} 5 & 2 & - & 7 & + & 4 & - & 15 \\ & & & 10 & + & 15 & + & 95 \\ \hline & 2 & + & 3 & + & 19 & + & 80 \end{array}$$

Observe that here there are 3 multiplications and 3 additions. In general, evaluating a polynomial of degree n by Horner's method would require approximately

$$n \text{ multiplications} \qquad \text{and} \qquad n \text{ additions}$$

Clearly Horner's method (*b*) is more efficient than the direct method (*a*).

EXAMPLE 3.11 (Greatest Common Divisor) Let a and b be positive integers with, say, $b < a$; and suppose we want to find $d = \text{GCD}(a, b)$, the greatest common divisor of a and b. This can be done in the following two ways.

(*a*) (***Direct Method***): Here we find all the divisors of a, say by testing all the numbers from 2 to $a/2$, and all the divisors of b. Then we pick the largest common divisor. For example, suppose $a = 258$ and $b = 60$. The divisors of a and b follow:

$$\begin{aligned} a &= 258; \quad \text{divisors:} \quad 1, \quad 2, \quad 3, \quad 6, \quad 86, \quad 129, \quad 258 \\ b &= \ 60; \quad \text{divisors;} \quad 1, \quad 2, \quad 3, \quad 4, \quad 5, \quad 6, \quad 10, \quad 12, \quad 15, \quad 20, \quad 30, \quad 60 \end{aligned}$$

Accordingly, $d = \text{GCD}(258, 60) = 6$.

(*b*) (***Euclidean Algorithm***): Here we divide a by b to obtain a remainder r_1. (Note $r_1 < b$.) Then we divide b by the remainder r_1 to obtain a second remainder r_2. (Note $r_2 < r_1$.) Next we divide r_1 by r_2 to obtain a third remainder r_3. (Note $r_3 < r_2$.) We continue dividing r_k by r_{k+1} to obtain a remainder r_{k+2}. Since

$$a > b > r_1 > r_2 > r_3 \ldots \qquad (*)$$

eventually we obtain a remainder $r_m = 0$. Then $r_{m-1} = \text{GCD}\ (a, b)$. For example, suppose $a = 258$ and $b = 60$. Then:

(1) Dividing $a = 258$ by $b = 60$ yields the remainder $r_1 = 18$.
(2) Dividing $b = 60$ by $r_1 = 18$ yields the remainder $r_2 = 6$.
(3) Dividing $r_1 = 18$ by $r_2 = 6$ yields the remainder $r_3 = 0$.

Thus $r_2 = 6 = \text{GCD}(258, 60)$.

The Euclidean algorithm is a very efficient way to find the greatest common divisor of two positive integers a and b. The fact that the algorithm ends follows from $(*)$. The fact that the algorithm yields $d = \text{GCD}(a, b)$ is not obvious; it is discussed in Section 11.6.

3.9 COMPLEXITY OF ALGORITHMS

The analysis of algorithms is a major task in computer science. In order to compare algorithms, we must have some criteria to measure the efficiency of our algorithms. This section discusses this important topic.

Suppose M is an algorithm, and suppose n is the size of the input data. The time and space used by the algorithm are the two main measures for the efficiency of M. The time is measured by counting the number of "key operations"; for example:

(a) In sorting and searching, one counts the number of comparisons.
(b) In arithmetic, one counts multiplications and neglects additions.

Key operations are so defined when the time for the other operations is much less than or at most proportional to the time for the key operations. The space is measured by counting the maximum of memory needed by the algorithm.

The *complexity* of an algorithm M is the function $f(n)$ which gives the running time and/or storage space requirement of the algorithm in terms of the size n of the input data. Frequently, the storage space required by an algorithm is simply a multiple of the data size. Accordingly, unless otherwise stated or implied, the term "complexity" shall refer to the running time of the algorithm.

The complexity function $f(n)$, which we assume gives the running time of an algorithm, usually depends not only on the size n of the input data but also on the particular data. For example, suppose we want to search through an English short story TEXT for the first occurrence of a given 3-letter word W. Clearly, if W is the 3-letter word "the", then W likely occurs near the beginning of TEXT, so $f(n)$ will be small. On the other hand, if W is the 3-letter word "zoo", then W may not appear in TEXT at all, so $f(n)$ will be large.

The above discussion leads us to the question of finding the complexity function $f(n)$ for certain cases. The two cases one usually investigates in complexity theory are as follows:

(1) *Worst case*: The maximum value of $f(n)$ for any possible input.
(2) *Average case*: The expected value of $f(n)$.

The analysis of the average case assumes a certain probabilistic distribution for the input data; one possible assumption might be that the possible permutations of a data set are equally likely. The average case also uses the following concept in probability theory. Suppose the numbers $n_1, n_2, \ldots, n_k$ occur with respective probabilities $p_1, p_2, \ldots, p_k$. Then the *expectation* or *average value* E is given by

$$E = n_1p_1 + n_2p_2 + \ldots + n_kp_k$$

These ideas are illustrated below.

Linear Search

Suppose a linear array DATA contains n elements, and suppose a specific ITEM of information is given. We want either to find the location LOC of ITEM in the array DATA, or to send some message, such as LOC = 0, to indicate that ITEM does not appear in DATA. The linear search algorithm solves this problem by comparing ITEM, one by one, with each element in DATA. That is, we compare ITEM with DATA[1], then DATA[2], and so on, until we find LOC such that ITEM = DATA[LOC].

The complexity of the search algorithm is given by the number C of comparisons between ITEM and DATA[K]. We seek $C(n)$ for the worst case and the average case.

(1) ***Worst Case***: Clearly the worst case occurs when ITEM is the last element in the array DATA or is not there at all. In either situation, we have

$$C(n) = n$$

Accordingly, $C(n) = n$ is the worst-case complexity of the linear search algorithm.

(2) ***Average Case***: Here we assume that ITEM does appear in DATA, and that is is equally likely to occur at any position in the array. Accordingly, the number of comparisons can be any of the numbers $1, 2, 3, \ldots, n$, and each number occurs with probability $p = 1/n$. Then

$$\begin{aligned} C(n) &= 1 \cdot \frac{1}{n} + 2 \cdot \frac{1}{n} + \cdots + n \cdot \frac{1}{n} \\ &= (1 + 2 + \cdots + n) \cdot \frac{1}{n} \\ &= \frac{n(n+1)}{2} \cdot \frac{1}{n} = \frac{n+1}{2} \end{aligned}$$

This agrees with our intuitive feeling that the average number of comparisons needed to find the location of ITEM is approximately equal to half the number of elements in the DATA list.

Remark: The complexity of the average case of an algorithm is usually much more complicated to analyze than that of the worst case. Moreover, the probabilistic distribution that one assumes for the average case may not actually apply to real situations. Accordingly, unless otherwise stated or implied, the complexity of an algorithm shall mean the function which gives the running time of the worst case in terms of the input size. This is not too strong an assumption, since the complexity of the average case for many algorithms is proportional to the worst case.

Rate of Growth; Big *O* Notation

Suppose M is an algorithm, and suppose n is the size of the input data. Clearly the complexity $f(n)$ of M increases as n increases. It is usually the rate of increase of $f(n)$ that we want to examine. This is usually done by comparing $f(n)$ with some standard function, such as

$$\log_2 n, \quad n, \quad n \log_2 n, \quad n^2, \quad n^3, \quad 2^n$$

The rates of growth for these standard functions are indicated in Fig. 3-6, which gives their approximate values for certain values of n. Observe that the functions are listed in the order of their rates of growth: the logarithmic function $\log_2 n$ grows most slowly, the exponential function 2^n grows most rapidly, and the polynomial functions n^c grow according to the exponent c.

n \ $g(n)$	$\log n$	n	$n \log n$	n^2	n^3	2^n
5	3	5	15	25	125	32
10	4	10	40	100	10^3	10^3
100	7	100	700	10^4	10^6	10^{30}
1000	10	10^3	10^4	10^6	10^9	10^{300}

Fig. 3-6 Rate of growth of standard functions.

The way we compare our complexity function $f(n)$ with one of the standard functions is to use the functional "big O" notation which we formally define below.

Definition: Let $f(x)$ and $g(x)$ be arbitrary functions defined on **R** or a subset of **R**. We say "$f(x)$ is of order $g(x)$", written

$$f(x) = O(g(x))$$

if there exists a real number k and a positive constant C such that, for all $x > k$, we have

$$|f(x)| \leq C|g(x)|$$

We also write

$$f(x) = h(x) + O(g(x)) \qquad \text{when} \qquad f(x) - h(x) = O(g(x))$$

(The above is called the "big O" notation since $f(x) = o(g(x))$ has an entirely different meaning.)

Consider now a polynomial $P(x)$ of degree m. Then we show in Problem 3.27 that $P(x) = O(x^m)$. Thus, for example,

$$7x^2 - 9x + 4 = O(x^2) \qquad \text{and} \qquad 8x^3 - 576x^2 + 832x - 248 = O(x^3)$$

Complexity of Well-known Algorithms

Assuming $f(n)$ and $g(n)$ are functions defined on the positive integers, then

$$f(n) = O(g(n))$$

means that $f(n)$ is bounded by a constant multiple of $g(n)$ for almost all n.

To indicate the convenience of this notation, we give the complexity of certain well-known searching and sorting algorithms in computer science:

(*a*) Linear search: $O(n)$
(*b*) Binary search: $O(\log n)$
(*c*) Bubble sort: $O(n^2)$
(*d*) Merge-sort: $O(n \log n)$

Solved Problems

FUNCTIONS

3.1. State whether or not each diagram in Fig. 3-7 defines a function from $A = \{a, b, c\}$ into $B = \{x, y, z\}$.

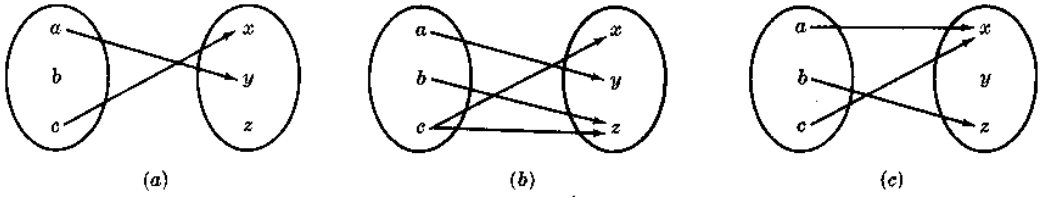


Fig. 3-7

(*a*) No. There is nothing assigned to the element $b \in A$.

(*b*) No. Two elements, x and z, are assigned to $c \in A$.

(*c*) Yes.

3.2. Let $X = \{1, 2, 3, 4\}$. Determine whether or not each relation below is a function from X into X.

(*a*) $f = \{(2, 3), (1, 4), (2, 1)(3, 2), (4, 4)\}$.

(*b*) $g = \{(3, 1), (4, 2), (1, 1)\}$.

(*c*) $h = \{(2, 1), (3, 4), (1, 4), (2, 1), (4, 4)\}$.

Recall that a subset f of $X \times X$ is a function $f: X \to X$ if and only if each $a \in X$ appears as the first coordinate in exactly one ordered pair in f.

(*a*) No. Two different ordered pairs (2, 3) and (2, 1) in f have the same number 2 as their first coordinate.

(*b*) No. The element $2 \in X$ does not appear as the first coordinate in any ordered pair in g.

(*c*) Yes. Although $2 \in X$ appears as the first coordinate in two ordered pairs in h, these two ordered pairs are equal.

3.3. Let A be the set of students in a school. Determine which of the following assignments defines a function on A.

(*a*) To each student assign his age.

(*b*) To each student assign his teacher.

(*c*) To each student assign his sex.

(*d*) To each student assign his spouse.

A collection of assignments is a function on A if and only if each element a in A is assigned exactly in one element. Thus:

(*a*) Yes, because each student has one and only one age.

(*b*) Yes, if each student has only one teacher; no, if any student has more than one teacher.

(*c*) Yes.

(*d*) No, if any student is not married; yes otherwise.

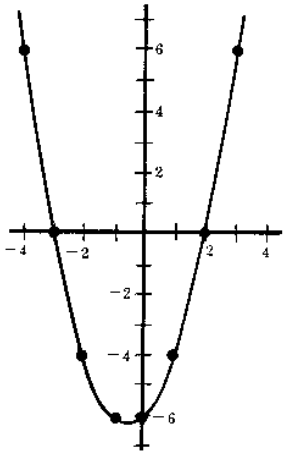
3.4. Sketch the graph of:

(*a*) $f(x) = x^2 + x - 6$

(*b*) $g(x) = x^3 - 3x^2 - x + 3$

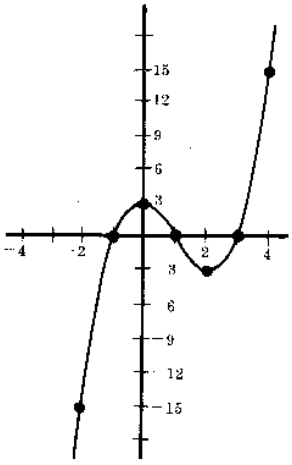
Set up a table of values for x and then find the corresponding values of the function. Since the functions are polynomials, plot the points in a coordinate diagram and then draw a smooth continuous curve through the points. See Fig. 3-8.

x	$f(x)$
−4	6
−3	0
−2	−4
−1	−6
0	−6
1	−4
2	0
3	6



Graph of f

x	$g(x)$
−2	−15
−1	0
0	3
1	0
2	−3
3	0
4	15



Graph of g

Fig. 3-8

3.5. Let the functions f: $A \to B$ and g: $B \to C$ be defined by Fig. 3-9. Find the composition function $g \circ f$: $A \to C$.

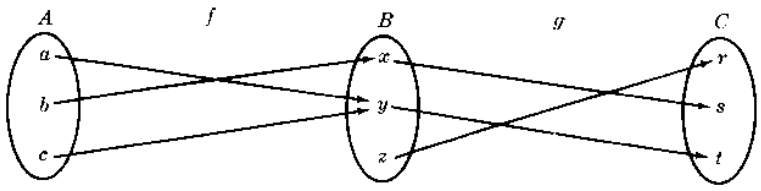


Fig. 3-9

We use the definition of the composition function to compute:

$$(g \circ f)(a) = g(f(a)) = g(y) = t$$
$$(g \circ f)(b) = g(f(b)) = g(x) = s$$
$$(g \circ f)(c) = g(f(c)) = g(y) = t$$

Note that we arrive at the same answer if we "follow the arrows" in the diagram:

$$a \to y \to t, \qquad b \to x \to s, \qquad c \to y \to t$$

3.6. Let the functions f and g be defined by $f(x) = 2x + 1$ and $g(x) = x^2 - 2$. Find the formula defining the composition function $g \circ f$.

Compute $g \circ f$ as follows: $(g \circ f(x) = g(f(x)) = g(2x + 1) = (2x + 1)^2 - 2 = 4x^2 + 4x - 1$.

Observe that the same answer can be found by writing

$$y = f(x) = 2x + 1 \qquad \text{and} \qquad z = g(y) = y^2 - 2$$

and then eliminating y from both equations:

$$z = y^2 - 2 = (2x + 1)^2 - 2 = 4x^2 + 4x - 1$$

ONE-TO-ONE, ONTO, AND INVERTIBLE FUNCTIONS

3.7. Determine if each function is one-to-one.

(*a*) To each person on the earth assign the number which corresponds to his age.
(*b*) To each country in the world assign the latitude and longitude of its capital.
(*c*) To each book written by only one author assign the author.
(*d*) To each country in the world which has a prime minister assign its prime minister.

(*a*) No. Many people in the world have the same age.
(*b*) Yes.
(*c*) No. There are different books with the same author.
(*d*) Yes. Different countries in the world have different prime ministers.

3.8. Let the functions f: $A \to B$, g: $B \to C$, and h: $C \to D$ be defined by Fig. 3-10.

(*a*) Determine if each function is onto.
(*b*) Find the composition function $h \circ g \circ f$.

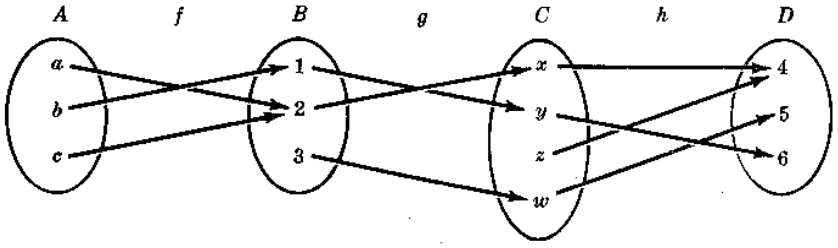


Fig. 3-10

(*a*) The function f: $A \to B$ is not onto since $3 \in B$ is not the image of any element in A.
The function g: $B \to C$ is not onto since $z \in C$ is not the image of any element in B.
The function h: $C \to D$ is onto since each element in D is the image of some element of C.

(*b*) Now $a \to 2 \to x \to 4$, $b \to 1 \to y \to 6$, $c \to 2 \to x \to 4$. Hence $h \circ g \circ f = \{(a,4),(b,6),(c,4)\}$.

3.9. Consider functions f: $A \to B$ and g: $B \to C$. Prove the following:

(*a*) If f and g are one-to-one, then the composition function $g \circ f$ is one-to-one.

(*b*) If f and g are onto functions, then $g \circ f$ is an onto function.

(*a*) Suppose $(g \circ f)(x) = (g \circ f)(y)$; then $g(f(x)) = g(f(y))$. Hence $f(x) = f(y)$ because g is one-to-one. Furthermore, $x = y$ since f is one-to-one. Accordingly, $g \circ f$ is one-to-one.

(*b*) Let c be any arbitrary element of C. Since g is onto, there exists a $b \in B$ such that $g(b) = c$. Since f is onto, there exists an $a \in A$ such that $f(a) = b$. But then

$$(g \circ f)(a) = g(f(a)) = g(b) = c$$

Hence each $c \in C$ is the image of some element $a \in A$. Accordingly, $g \circ f$ is an onto function.

3.10. Let f: $\mathbf{R} \to \mathbf{R}$ be defined by $f(x) = 2x - 3$. Now f is one-to-one and onto; hence f has an inverse function f^{-1}. Find a formula for f^{-1}.

Let y be the image of x under the function f:

$$y = f(x) = 2x - 3$$

Consequently, x will be the image of y under the inverse function f^{-1}. Solve for x in terms of y in the above equation:

$$x = (y + 3)/2$$

Then $f^{-1}(y) = (y + 3)/2$. Replace y by x to obtain

$$f^{-1}(x) = \frac{x + 3}{2}$$

which is the formula for f^{-1} using the usual independent variable x.

3.11. Prove the following generalization of DeMorgan's law: For any class of sets $\{A_i\}$, we have

$$(\cup_i A_i)^c = \cap_i A_i^c$$

We have:

$$x \in (\cup_i A_i)^c \quad \text{iff } x \notin \cup_i A_i, \quad \text{iff } \forall_i \in I, x \notin A_i, \quad \text{iff } \forall_i \in I, x \in A_i^c, \quad \text{iff } x \in \cap_i A_i^c$$

Therefore, $(\cup_i A_i)^c = \cap_i A_i^c$. (Here we have used the logical notations iff for "if and only if" and $\forall$ for "for all".)

CARDINALITY

3.12. Find the cardinal number of each set.

(*a*) $A = \{a, b, c, \ldots, y, z\}$ (*d*) $D = \{10, 20, 30, 40, \ldots\}$

(*b*) $B = \{1, -3, 5, 11, -28\}$ (*e*) $E = \{6, 7, 8, 9, \ldots\}$

(*c*) $C = \{x: x \in \mathbf{N}, x^2 = 5\}$

(*a*) $|A| = 26$ since there are 26 letters in the English alphabet.

(*b*) $|B| = 5$.

(*c*) $|C| = 0$ since there is no positive integer whose square is 5, i.e., since C is empty.

(*d*) $|D| = \aleph_0$ because $f: \mathbf{N} \to D$, defined by $f(n) = 10n$, is a one-to-one correspondence between $\mathbf{N}$ and D.

(*e*) $|E| = \aleph_0$ because $g: \mathbf{N} \to E$, defined by $g(n) = n + 5$ is a one-to-one correspondence between $\mathbf{N}$ and E.

3.13. Show that the set $\mathbf{Z}$ of integers has cardinality $\aleph_0$.

The following diagram shows a one-to-one correspondence between $\mathbf{N}$ and $\mathbf{Z}$:

$$\begin{array}{lcccccccccc} \mathbf{N} = & 1 & 2 & 3 & 4 & & 5 & 6 & 7 & 8 & \ldots \\ & \downarrow & \downarrow & \downarrow & \downarrow & & \downarrow & \downarrow & \downarrow & \downarrow & \ldots \\ \mathbf{Z} = & 0 & 1 & -1 & 2 & -2 & 3 & -3 & 4 & \ldots \end{array}$$

That is, the following function $f: \mathbf{N} \to \mathbf{Z}$ is one-to-one and onto:

$$f(n) = \begin{cases} n/2 & \text{if } n \text{ is even} \\ (1-n)/2 & \text{if } n \text{ is odd} \end{cases}$$

Accordingly, $|\mathbf{Z}| = |\mathbf{N}| = \aleph_0$.

3.14. Let $A_1, A_2, \ldots$ be a countable number of finite sets. Prove that the union $S = \cup_i A_i$ is countable.

Essentially, we list the elements of A_1, then we list the elements of A_2 which do not belong to A_1, then we list the elements of A_3 which do not belong to A_1 or A_2, i.e., which have not already been listed, and so on. Since the A_i are finite, we can always list the elements of each set. This process is done formally as follows.

First we define sets $B_1, B_2, \ldots$ where B_i contains the elements of A_i which do not belong to preceding sets, i.e., we define

$$B_1 = A_1 \qquad \text{and} \qquad B_k = A_k \backslash (A_1 \cup A_2 \cup \cdots \cup A_{k-1})$$

Then the B_i are disjoint and $S = \cup_i B_i$. Let $b_{i1}, b_{i2}, \ldots, b_{im_i}$ be the elements of B_i. Then $S = \{b_{ij}\}$. Let $f: S \to \mathbf{N}$ be defined as follows:

$$f(b_{ij}) = m_1 + m_2 + \cdots + m_{i-1} + j$$

If S is finite, then S is countable. If S is infinite then f is a one-to-one correspondence between S and $\mathbf{N}$. Thus S is countable.

3.15. Prove Theorem 3.2: A countable union of countable sets is countable.

Suppose $A_1, A_2, A_3, \ldots$ are a countable number of countable sets. In particular, suppose $a_{i1}, a_{i2}, a_{i3}, \ldots$ are the elements of A_i. Define sets $B_2, B_3, B_4, \ldots$ as follows:

$$B_k = \{a_{ij}: i + j = k\}$$

For example, $B_6 = \{a_{15}, a_{24}, a_{33}, a_{42}, a_{51}\}$. Observe that each B_k is finite and

$$S = \cup_i A_i = \cup_k B_k$$

By the preceding problem $\cup_k B_k$ is countable. Hence $S = \cup_i A_i$ is countable and the theorem is proved.

3.16. Prove Theorem 3.3: The set I of all real numbers between 0 and 1 inclusive is uncountable.

The set I is clearly infinite, since it contains $1, \frac{1}{2}, \frac{1}{3}, \ldots$. Suppose I is denumberable. Then there exists a one-to-one correspondence $f: \mathbf{N} \to I$. Let $f(1) = a_1, f(2) = a_2, \ldots$; that is, $I = \{a_1, a_2, a_3, \ldots\}$. We list the elements $a_1, a_2, \ldots$ in a column and express each in its decimal expansion:

$$\begin{aligned} a_1 &= 0.x_{11}x_{12}x_{13}x_{14}\ldots \\ a_2 &= 0.x_{21}x_{22}x_{23}x_{24}\ldots \\ a_3 &= 0.x_{31}x_{32}x_{33}x_{34}\ldots \\ a_4 &= 0.x_{41}x_{42}x_{43}x_{44}\ldots \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{aligned}$$

where $x_{ij} \in \{0, 1, 2, \ldots, 9\}$. (For those numbers which can be expressed in two different decimal expansions, e.g., $0.200\,0000\ldots = 0.199\,9999\ldots$, we choose the expansion which ends with nines.)

Let $b = 0.y_1y_2y_3y_4\ldots$ be the real number obtained as follows:

$$y_i = \begin{cases} 1 & \text{if } x_{ii} \neq 1 \\ 2 & \text{if } x_{ii} = 1 \end{cases}$$

Now $b \in I$. But

$$\begin{aligned} &b \neq a_1 \text{ because } y_1 \neq x_{11} \\ &b \neq a_2 \text{ because } y_2 \neq x_{22} \\ &b \neq a_3 \text{ because } y_3 \neq x_{33} \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{aligned}$$

Therefore b does not belong to $I = \{a_1, a_2, \ldots\}$. This contradicts the fact that $b \in I$. Hence the assumption that I is denumerable must be false, so I is uncountable.

SPECIAL MATHEMATICAL FUNCTIONS

3.17. Find: (*a*) $\lfloor 7.5 \rfloor$; $\lfloor -7.5 \rfloor, \lfloor -18 \rfloor$; (*b*) $\lceil 7.5 \rceil, \lceil -7.5 \rceil, \lceil -18 \rceil$.

(*a*) By definition, $\lfloor x \rfloor$ denotes the greatest integer that does not exceed x, hence $\lfloor 7.5 \rfloor = 7, \lfloor -7.5 \rfloor = -8$, $\lfloor -18 \rfloor = -18$.

(*b*) By definition, $\lceil x \rceil$ denotes the least integer that is not less than x, hence $\lceil 7.5 \rceil = 8, \lceil -7.5 \rceil = -7$, $\lceil -18 \rceil = -18$.

3.18. Find: (*a*) $25 \pmod 7$; (*b*) $25 \pmod 5$; (*c*) $-35 \pmod{11}$; (*d*) $-3 \pmod 8$.

When k is positive, simply divide k by the modulus M to obtain the remainder r. Then $r = k \pmod M$. If k is negative, divide $|k|$ by M to obtain the remainder r'. Then $k \pmod M = M - r'$ (when $r' \neq 0$). Thus:

(*a*) $25 \pmod 7 = 4$, (*c*) $-35 \pmod{11} = 11 - 2 = 9$,

(*b*) $25 \pmod 5 = 0$, (*d*) $-3 \pmod 8 = 8 - 3 = 5$.

3.19. Using arithmetic modulo $M = 15$, evaluate: (*a*) $9 + 13$; (*b*) $7 + 11$; (*c*) $4 - 9$; (*d*) $2 - 10$.

Use $a + M \equiv a \pmod M$:

(*a*) $9 + 13 = 22 \equiv 22 - 15 = 7$. (*c*) $4 - 9 = -5 \equiv -5 + 15 = 10$.

(*b*) $7 + 11 = 18 \equiv 18 - 15 = 3$. (*d*) $2 - 10 = -8 \equiv -8 + 15 = 7$.

3.20. Simplify: (*a*) $\dfrac{n!}{(n-1)!}$; (*b*) $\dfrac{(n+2)!}{n!}$.

(*a*) $\dfrac{n!}{(n-1)!} = \dfrac{n(n-1)(n-2)\cdots 3\cdot 2\cdot 1}{(n-1)(n-2)\cdots 3\cdot 2\cdot 1} = n$ or, simply, $\dfrac{n!}{(n-1)!} = \dfrac{n(n-1)!}{(n-1)!} = n$.

(*b*) $$\frac{(n+2)!}{n!} = \frac{(n+2)(n+1)n(n-1)(n-2)\cdots 3\cdot 2\cdot 1}{n(n-1)(n-2)\cdots 3\cdot 2\cdot 1} = (n+2)(n+1) = n^2+3n+2$$

or simply, $$\frac{(n+2)!}{n!} = \frac{(n+2)(n+1)n!}{n!} = (n+2)(n+1) = n^2+3n+2.$$

3.21. Evaluate: (*a*) $\log_2 8$; (*b*) $\log_2 64$; (*c*) $\log_{10} 100$; (*d*) $\log_{10} 0.001$.

(*a*) $\log_2 8 = 3$ since $2^3 = 8$. (*c*) $\log_{10} 100 = 2$ since $10^2 = 100$.

(*b*) $\log_2 64 = 6$ since $2^6 = 64$. (*d*) $\log_{10} 0.001 = -3$ since $10^{-3} = 0.001$.

Remark: Frequently, logarithms are expressed using approximate values. For example, using tables or calculators, we obtain

$$\log_{10} 300 = 2.4771 \qquad \text{and} \qquad \log_e 40 = 3.6889$$

as approximate answers. (Here $e = 2.718281\ldots$.)

RECURSIVE FUNCTIONS

3.22. Let a and b be positive integers, and suppose Q is defined recursively as follows:

$$Q(a,b) = \begin{cases} 0 & \text{if } a < b \\ Q(a-b,b)+1 & \text{if } b \le a \end{cases}$$

(*a*) Find: (i) $Q(2,5)$, (ii) $Q(12,5)$.

(*b*) What does this function Q do? Find $Q(5861,7)$.

(*a*) (i) $Q(2, 5) = 0$ since $2 < 5$.

(ii) $$\begin{aligned} Q(12, 5) &= Q(7, 5) + 1 \\ &= [Q(2, 5) + 1] + 1 = Q(2, 5) + 2 \\ &= 0 + 2 = 2. \end{aligned}$$

(*b*) Each time b is subtracted from a, the value of Q is increased by 1. Hence $Q(a,b)$ finds the quotient when a is divided by b. Thus $Q(5861,7) = 837$.

3.23. Let n denote a positive integer. Suppose a function L is defined recursively as follows:

$$L(n) = \begin{cases} 0 & \text{if } n = 1 \\ L(\lfloor n/2 \rfloor) + 1 & \text{if } n > 1 \end{cases}$$

Find $L(25)$ and describe what this function does.

Find $L(25)$ recursively as follows:

$$\begin{aligned} L(25) &= L(12) + 1 \\ &= [L(6) + 1] + 1 = L(6) + 2 \\ &= [L(3) + 1] + 2 = L(3) + 3 \\ &= [L(1) + 1] + 3 = L(1) + 4 = 0 + 4 = 4 \end{aligned}$$

Each time n is divided by 2, then the value of L is increased by 1. Hence L is the greatest integer such that

$$2^L \le n$$

Accordingly, $$L(n) = \lfloor \log_2 n \rfloor$$

3.24. Use the definition of the Ackermann function to find $A(1,3)$.

We have the following 15 steps:

(1) $A(1,3) = A(0, A(1,2))$
(2) $A(1,2) = A(0, A(1,1))$
(3) $A(1,1) = A(0, A(1,0))$
(4) $A(1,0) = A(0,1)$
(5) $A(0,1) = 1 + 1 = 2$
(6) $A(1,0) = 2$
(7) $A(1,1) = A(0,2)$
(8) $A(0,2) = 2 + 1 = 3$
(9) $A(1,1) = 3$
(10) $A(1,2) = A(0,3)$
(11) $A(0,3) = 3 + 1 = 4$
(12) $A(1,2) = 4$
(13) $A(1,3) = A(0,4)$
(14) $A(0,4) = 4 + 1 = 5$
(15) $A(1,3) = 5$

The forward indention indicates that we are postponing an evaluation and are recalling the definition, and the backward indention indicates that we are backtracking. Observe that (*a*) of the definition is used in Steps 5, 8, 11 and 14; (*b*) in Step 4; and (*c*) in Steps 1, 2 and 3. In the other steps we are backtracking with substitutions.

MISCELLANEOUS PROBLEMS

3.25. Find the domain D of each of the following real-valued functions of a real variable:

(*a*) $f(x) = \dfrac{1}{x-2}$. (*c*) $f(x) = \sqrt{25 - x^2}$.

(*b*) $f(x) = x^2 - 3x - 4$. (*d*) $f(x) = x^2$ where $0 \le x \le 2$.

When a real-valued function of a real variable is given by a formula $f(x)$, then the domain D consists of the largest subset of $\mathbf{R}$ for which $f(x)$ has meaning and is real, unless otherwise specified.

(*a*) f is not defined for $x - 2 = 0$, i.e., for $x = 2$; hence $D - \mathbf{R}\backslash\{2\}$.

(*b*) f is defined for every real number; hence $D = \mathbf{R}$.

(*c*) f is not defined when $25 - x^2$ is negative; hence $D = [-5, 5] = \{x: -5 \le x \le 5\}$.

(*d*) Here, the domain of f is explicitly given as $D = \{x: 0 \le x \le 2\}$.

3.26. For any $n \in \mathbf{N}$, let $D_n = (0, 1/n)$, the open interval from 0 to $1/n$. Find:

$$(a)\ D_3 \cup D_7; \quad (b)\ D_3 \cap D_{20}; \quad (c)\ D_s \cup D_t; \quad (d)\ D_s \cap D_t.$$

(*a*) Since $(0, 1/3)$ is a superset of $(0, 1/7)$, $D_3 \cup D_7 = D_3$.

(*b*) Since $(0, 1/20)$ is a subset of $(0, 1/3)$, $D_3 \cap D_{20} = D_{20}$.

(*c*) Let $m = \min(s, t)$, that is, the smaller of the two numbers s and t; then D_m is equal to D_s, or D_t and contains the other as a subset. Hence $D_s \cup D_t = D_m$.

(*d*) Let $M = \max(s, t)$, that is, the larger of the two numbers s and t; then $D_s \cap D_t = D_M$.

3.27. Suppose $P(n) = a_0 + a_1 n + a_2 n^2 + \cdots + a_m n^m$ has degree m. Prove $\mathrm{P(n)} = \mathrm{O}(n^m)$.

Let $b_0 = |a_0|, b_1 = |a_1|, \ldots, b_m = |a_m|$. Then, for $n \ge 1$,

$$P(n) \le b_0 + b_1 n + b_2 n^2 + \cdots + b_m n^m = \left(\frac{b_0}{n^m} + \frac{b_1}{n^{m-1}} + \cdots + b_m\right) n^m$$
$$\le (b_0 + b_1 + \cdots + b_m) n^m = M n^m$$

where $M = |a_0| + |a_1| + \cdots + |a_m|$. Hence $P(n) = O(n^m)$.

For example, $5x^3 + 3x = O(x^3)$ and $x^5 - 4\,000\,000x^2 = O(x^5)$.

3.28. Prove Theorem 3.4 (Cantor): $|A| < |\text{Power}(A)|$ (where $\text{Power}(A)$ is the power set of A).

The function $g: A \to \text{Power}(A)$ defined by $g(a) = \{a\}$ is clearly one-to-one; hence $|A| \leq |\text{Power}(A)|$.

If we show that $|A| \neq |\text{Power}(A)|$, then the theorem will follow. Suppose the contrary, that is, suppose $|A| = |\text{Power}(A)|$ and that $f: A \to \text{Power}(A)$ is a function which is both one-to-one and onto. Let $a \in A$ be called a "bad" element if $a \notin f(a)$, and let B be the set of bad elements. In other words,

$$B = \{x: x \in A,\ x \notin f(x)\}$$

Now B is a subset of A. Since $f: A \to \text{Power}(A)$ is onto, there exists $b \in A$ such that $f(b) = B$. Is b a "bad" element or a "good" element? If $b \in B$ then, by definition of B, $b \notin f(b) = B$, which is impossible. Likewise, if $b \notin B$ then $b \in f(b) = B$, which is also impossible. Thus the original assumption that $|A| = |\text{Power}(A)|$ has led to a contradiction. Hence the assumption is false, and so the theorem is true.

3.29. Prove the following equivalent formulation of the Schroeder-Bernstein Theorem 3.5: Suppose $X \supseteq Y \supseteq X_1$ and $X \simeq X_1$. Then $X \simeq Y$.

Since $X \simeq X_1$, there exists a one-to-one correspondence (bijection) $f: X \to X_1$. Since $X \supseteq Y$, the restriction of f to Y, which we also denote by f, is also one-to-one. Let $f(Y) = Y_1$. Then Y and Y_1 are equipotent,

$$X \supseteq Y \supseteq X_1 \supseteq Y_1$$

and $f: Y \to Y_1$ is bijective. But now $Y \supseteq X_1 \supseteq Y_1$ and $Y \simeq Y_1$. For similar reasons, X_1 and $f(X_1) = X_2$ are equipotent,

$$X \supseteq Y \supseteq X_1 \supseteq Y_1 \supseteq X_2$$

and $f: X_1 \to X_2$ is bijective. Accordingly, there exists equipotent sets X, X_1, $X_2, \ldots$ and equipotent sets $Y, Y_1, Y_2, \ldots$ such that

$$X \supseteq Y \supseteq X_1 \supseteq Y_1 \supseteq X_2 \supseteq Y_2 \supseteq X_3 \supseteq Y_3 \supseteq \cdots$$

and $f: X_k \to X_{k+1}$ and $f: Y_k \to Y_{k+1}$ are bijective.

Let

$$B = X \cap Y \cap X_1 \cap Y_1 \cap X_2 \cap Y_2 \cap \cdots$$

Then

$$X = (X \backslash Y) \cup (Y \backslash X_1) \cup (X_1 \backslash Y_1) \cup \cdots \cup B$$
$$Y = (Y \backslash X_1) \cup (X_1 \backslash Y_1) \cup (Y_1 \backslash X_2) \cup \cdots \cup B$$

Furthermore, $X \backslash Y$, $X_1 \backslash Y_1$, $X_2 \backslash Y_2, \ldots$ are equipotent. In fact, the function

$$f: (X_k \backslash Y_k) \to (X_{k+1} \backslash Y_{k+1})$$

is one-to-one and onto.

Consider the function $g: X \to Y$ defined by the diagram in Fig. 3-11. That is,

$$g(x) = \begin{cases} f(x) & \text{if } x \in X_k \backslash Y_k \text{ or } x \in X \backslash Y \\ x & \text{if } x \in Y_k \backslash X_k \text{ or } x \in B \end{cases}$$

Then g is one-to-one and onto. Therefore $X \simeq Y$.

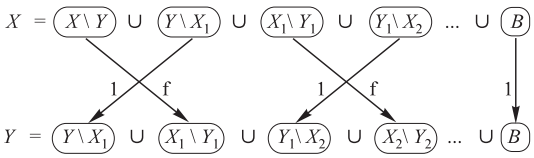


Fig. 3-11

Supplementary Problems

FUNCTIONS

3.30. Let $W = \{a, b, c, d\}$. Determine whether each set of ordered pairs is a function from W into W.

(*a*) $\{(b,a),(c,d),(d,a),(c,d),(a,d)\}$ (*c*) $\{(a,b),(b,b),(c,b),(d,b)\}$

(*b*) $\{(d,d),(c,a),(a,b),(d,b)\}$ (*d*) $\{(a,a),(b,a),(a,b),(c,d)\}$

3.31. Let the function g assign to each name in the set {Britt, Martin, David, Alan, Rebecca} the number of different letters needed to spell the name. Write g as a set of ordered pairs.

3.32. Let $W = \{1, 2, 3, 4\}$ and let g: $W \to W$ be defined by Fig. 3-12. (*a*) Write g as a set of ordered pairs. (*b*) Find the image of g. (*c*) Write the composition function $g \circ g$ as a set of ordered pairs.

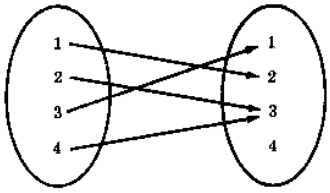


Fig. 3-12

3.33. Let $V = \{1, 2, 3, 4\}$ and let

$$f = \{(1,3),(2,1),(3,4),(4,3)\} \quad \text{and} \quad g = \{(1,2),(2,3),(3,1),(4,1)\}$$

Find: (*a*) $f \circ g$; (*b*) $g \circ f$; (*c*) $f \circ f$.

3.34. Let f: $\mathbf{R} \to \mathbf{R}$ be defined by $f(x) = 3x - 7$. Find a formula for the inverse function f^{-1}: $\mathbf{R} \to \mathbf{R}$.

PROPERTIES OF FUNCTIONS

3.35. Prove: If f: $A \to B$ and g: $B \to A$ satisfy $g \circ f = 1_A$, then f is one-to-one and g is onto.

3.36. Prove Theorem 3.1: A function f: $A \to B$ is invertible if and only if f is both one-to-one and onto.

3.37. Prove: If f: $A \to B$ is invertible with inverse function f^{-1}: $B \to A$, then $f^{-1} \circ f = 1_A$ and $f \circ f^{-1} = 1_B$.

3.38. For each positive integer n in $\mathbf{N}$, let A_n be the following subset of the real numbers $\mathbf{R}$:

$$A_n = (0, 1/n) = \{x\colon 0 < x < 1/n\}$$

Find: (*a*) $A_c \cup A_8$ (*c*) $\cup(A_i\colon i \in J)$ (*e*) $\cup(A_i\colon i \in K)$

(*b*) $A_3 \cap A_7$ (*d*) $\cap(A_i\colon i \in J)$ (*f*) $\cap(A_i\colon i \in K)$

where J is a finite subset of N and K is an infinite subset of $\mathbf{N}$.

3.39. Consider an indexed class of sets $\{A_i\colon i \in I\}$, a set B and an index i_0 in I. Prove:

(*a*) $B \cap (\cup_i A_i) = \cup_i (B \cap A_i)$.

(*b*) $\cap(A_i\colon i \in I) \subseteq A_{i_0} \subseteq \cup(A_i\colon i \in I)$.

3.40. For each positive integer n in **N**, let D_n be the following subset of **N**:

$$D_n = \{n, 2n, 3n, 4n, \ldots\} = \{\text{multiples of } n\}$$

(*a*) Find: (1) $D_2 \cap D_7$; (2) $D_6 \cap D_8$; (3) $D_3 \cup D_{12}$; (4) $D_3 \cap D_{12}$.

(*b*) Prove that $\cap(D_i: i \in J) = \varnothing$ where J is an infinite subset of **N**.

CARDINAL NUMBERS

3.41. Find the cardinal number of each set:

(*a*) {Monday, Tuesday, ..., Sunday}

(*b*) $\{x: x$ is a letter in the word "BASEBALL"$\}$

(*c*) $\{x: x^2 = 9, 2x = 8\}$

(*d*) The power set Power(A) of $A = \{1, 5, 7, 11\}$

(*e*) Collection of functions from $A = \{a, b, c\}$ into $B = \{1, 2, 3, 4\}$

(*f*) Set of relations on $A = \{a, b, c\}$

3.42. Prove that:

(*a*) Every infinite set A has a denumerable subset D.

(*b*) Each subset of a denumerable set is finite or denumerable.

(*c*) If A and B are denumerable, then $A \times B$ is denumerable.

(*d*) The set **Q** of rational numbers is denumerable.

3.43. Prove that: (*a*) $|A \times B| = |B \times A|$. (*b*) If $A \subseteq B$ then $|A| \leq |B|$. (*c*) If $|A| = |B|$ then $|P(A)| = |P(B)|$.

3.44. Find the cardinal number of each set: (*a*) the collection X of functions from $A = \{a, b, c, d\}$ into $B = \{1, 2, 3, 4, 5\}$; (*b*) the set Y of all relations on $A = \{a, b, c, d\}$.

SPECIAL FUNCTIONS

3.45. Find: (*a*) $\lfloor 13.2 \rfloor, \lfloor -0.17 \rfloor, \lfloor 34 \rfloor$; (*b*) $\lceil 13.2 \rceil, \lceil -0.17 \rceil, \lceil 34 \rceil$.

3.46. Find: (*a*) $10 \pmod 3$; (*b*) $200 \pmod{20}$; (*c*) $5 \pmod{12}$; (*d*) $29 \pmod 6$; (*e*) $-347 \pmod 6$; (*f*) $-555 \pmod{11}$.

3.47. Find: (*a*) $3! + 4!$; (*b*) $3!(3! + 2!)$; (*c*) $6!/5!$; (*d*) $30!/28!$.

3.48. Evaluate: (*a*) $\log_2 16$; (*b*) $\log_3 27$; (*c*) $\log_{10} 0.01$.

MISCELLANEOUS PROBLEMS

3.49. Prove: The set P of all polynomials

$$p(x) = a_0 + a_1 x + \cdots + a_m x^m$$

with integral coefficients, that is, where $a_0, a_1, \ldots, a_m$ are integers, is denumerable.

3.50. Let a and b be integers, and suppose $Q(a, b)$ is defined recursively by

$$Q(a,b) = \begin{cases} 5 & \text{if } a < b \\ Q(a-b,\ b+2) + a & \text{if } a \geq b \end{cases}$$

Find $Q(2,7),\ Q(5,3),$ and $Q(15,2)$.

Answers to Supplementary Problems

3.29. (*a*) No; (*b*) Yes; (*c*) No.

3.30. (*a*) Yes; (*b*) No; (*c*) Yes; (*d*) No.

3.31. $g = \{(\text{Britt}, 4), (\text{Martin}, 6), (\text{David}, 4), (\text{Alan}, 3), (\text{Rebecca}, 5)\}$

3.32. (*a*) $g = \{(1,2), (2,3), (3,1), (4,3)\}$; (*b*) $\{1,2,3\}$;
(*c*) $g \circ g = \{(1,3), (2,1), (3,2), (4,1)\}$.

3.33. (*a*) $\{(1,1), (2,4), (3,3), (4,3)$. (*b*) $\{(1,1), (2,2), (3,1), (4,1)$. (*c*) $\{(1,4), (2,3), (3,3), (4,4)$.

3.34. $f^{-1}(x) = \dfrac{x+7}{3}$

3.38. (*a*) A_5; (*b*) A_7; (*c*) A_r where r is the smallest integer in J; (*d*) A_s where s is the largest integer in J; (*e*) A_r where r is the smallest integer in K; (*f*) $\varnothing$.

3.40. (1) D_{14}; (2) D_{24}; (3) D_3; (4) D_{12}.

3.41. (*a*) 7; (*b*) 5; (*c*) 0; (*d*) 16; (*e*) $4^3 = 64$; (*f*) $2^9 = 512$.

3.44. (*a*) $5^4 = 625$; (*b*) $2^{16} = 65{,}536$.

3.45. (*a*) 13, −1, 34; (*b*) 14, 0, 34.

3.46. (*a*) 1; (*b*) 0; (*c*) 2; (*d*) 5. (*e*) $6 - 5 = 1$; (*f*) $11 - 5 = 6$.

3.47. (*a*) 30; (*b*) 48; (*c*) 6; (*d*) 870.

3.48. (*a*) 4; (*b*) 3; (*c*) −2.

3.49. *Hint*: Let P_k denote the set of all such polynomials $p(x)$ such that $m \leq k$ and each $|a_i| \leq m$. Then P_k is finite and $P = \cup_k P_k$.

3.50. $Q(2,7) = 5,\ Q(5,3) = 10,\ Q(15,2) = 42.$

© The McGraw–Hill Companies, 2004

Chapter 4

Logic and Propositional Calculus

4.1 INTRODUCTION

Many proofs in mathematics and many algorithms in computer science use logical expressions such as

"IF p THEN q" or "IF p_1 AND p_2, THEN q_1 OR q_2"

It is therefore necessary to know the cases in which these expressions are either TRUE or FALSE: what we refer to as the truth values of such expressions. We discuss these issues in this section.

We also investigate the truth value of quantified statements, which are statements which use the logical quantifiers "for every" and "there exists".

4.2 PROPOSITIONS AND COMPOUND PROPOSITIONS

A *proposition* (or *statement*) is a declarative sentence which is true or false, but not both. Consider, for example, the following eight sentences:

(i) Paris is in France.
(ii) $1 + 1 = 2$.
(iii) $2 + 2 = 3$.
(iv) London is in Denmark.
(v) $9 < 6$.
(vi) $x = 2$ is a solution of $x^2 = 4$.
(vii) Where are you going?
(viii) Do your homework.

All of them are propositions except (vii) and (viii). Moreover, (i), (ii), and (vi) are true, whereas (iii), (iv), and (v) are false.

Compound Propositions

Many propositions are *composite*, that is, composed of *subpropositions* and various connectives discussed subsequently. Such composite propositions are called *compound propositions*. A proposition is said to be *primitive* if it cannot be broken down into simpler propositions, that is, if it is not composite.

EXAMPLE 4.1

(*a*) "Roses are red and violets are blue" is a compound proposition with subpropositions "Roses are red" and "Violets are blue".

(*b*) "John is intelligent or studies every night" is a compound proposition with subpropositions "John is intelligent" and "John studies every night".

(*c*) The above propositions (i) through (vi) are all primitive propositions; they cannot be broken down into simpler propositions.

The fundamental property of a compound proposition is that its truth value is completely determined by the truth values of its subpropositions together with the way in which they are connected to form the compound propositions. The next section studies some of these connectives.

4.3 BASIC LOGICAL OPERATIONS

This section discusses the three basic logical operations of conjunction, disjunction, and negation which correspond, respectively, to the English words "and", "or", and "not".

Conjunction, $p \wedge q$

Any two propositions can be combined by the word "and" to form a compound proposition called the *conjunction* of the original propositions. Symbolically,

$$p \wedge q$$

read "p and q", denotes the conjunction of p and q. Since $p \wedge q$ is a proposition it has a truth value, and this truth value depends only on the truth values of p and q. Specifically:

Definition 4.1: If p and q are true, then $p \wedge q$ is true; otherwise $p \wedge q$ is false.

The truth value of $p \wedge q$ may be defined equivalently by the table in Fig. 4-1(a). Here, the first line is a short way of saying that if p is true and q is true, then $p \wedge q$ is true. The second line says that if p is true and q is false, then $p \wedge q$ is false. And so on. Observe that there are four lines corresponding to the four possible combinations of T and F for the two subpropositions p and q. Note that $p \wedge q$ is true only when both p and q are true.

EXAMPLE 4.2 Consider the following four statements:

(i) Paris is in France and $2 + 2 = 4$.
(ii) Paris is in France and $2 + 2 = 5$.
(iii) Paris is in England and $2 + 2 = 4$.
(iv) Paris is in England and $2 + 2 = 5$.

Only the first statement is true. Each of the other statements is false, since at least one of its substatements is false.

p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

(a) "p and q"

p	q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

(b) "p or q"

p	$\neg p$
T	F
F	T

(c) "not p"

Fig. 4-1

Disjunction, $p \vee q$

Any two propositions can be combined by the word "or" to form a compound proposition called the *disjunction* of the original propositions. Symbolically,

$$p \vee q$$

read "p or q", denotes the disjunction of p and q. The truth value of $p \vee q$ depends only on the truth values of p and q as follows.

Definition 4.2: If p and q are false, then $p \vee q$ is false; otherwise $p \vee q$ is true.

The truth value of $p \vee q$ may be defined equivalently by the table in Fig. 4-1(b). Observe that $p \vee q$ is false only in the fourth case when both p and q are false.

EXAMPLE 4.3 Consider the following four statements:

(i) Paris is in France or $2 + 2 = 4$.

(ii) Paris is in France or $2 + 2 = 5$.

(iii) Paris is in England or $2 + 2 = 4$.

(iv) Paris is in England or $2 + 2 = 5$.

Only the last statement (iv) is false. Each of the other statements is true since at least one of its substatements is true.

Remark: The English word "or" is commonly used in two distinct ways. Sometimes it is used in the sense of "p or q or both", i.e., at least one of the two alternatives occurs, as above, and sometimes it is used in the sense of "p or q but not both", i.e., exactly one of the two alternatives occurs. For example, the sentence "He will go to Harvard or to Yale" uses "or" in the latter sense, called the *exclusive disjunction*. Unless otherwise stated, "or" shall be used in the former sense. This discussion points out the precision we gain from our symbolic language: $p \vee q$ is defined by its truth table and *always* means "p and/or q".

Negation, $\neg p$

Given any proposition p, another proposition, called the *negation* of p, can be formed by writing "It is not the case that ..." or "It is false that ..." before p or, if possible, by inserting in p the word "not". Symbolically,

$$\neg p$$

read "not p", denotes the negation of p. The truth value of $\neg p$ depends on the truth value of p as follows.

Definition 4.3: If p is true, then $\neg p$ is false; and if p is false, then $\neg p$ is true.

The truth value of $\neg p$ may be defined equivalently by the table in Fig. 4-1(c). Thus the truth value of the negation of p is always the opposite of the truth value of p.

EXAMPLE 4.4 Consider the following six statements:

(a_1)	Paris is in France.	(b_1)	$2 + 2 = 5$.
(a_2)	It is not the case that Paris is in France.	(b_2)	It is not the case that $2 + 2 = 5$.
(a_3)	Paris is not in France.	(b_3)	$2 + 2 \neq 5$.

Then (a_2) and (a_3) are each the negation of (a_1); and (b_2) and (b_3) are each the negation of (b_1). Since (a_1) is true, (a_2) and (a_3) are false; and since (b_1) is false, (b_2) and (b_3) are true.

Remark: The logical notation for the connectives "and", "or", and "not" is not completely standardized. For example, some texts use:

$p \,\&\, q$, $p \cdot q$ or pq	for $p \wedge q$
$p + q$	for $p \vee q$
p', $\bar{p}$ or $\sim p$	for $\neg p$

4.4 PROPOSITIONS AND TRUTH TABLES

Let $P(p, q, \ldots)$ denote an expression constructed from logical variables p, q, ..., which take on the value TRUE (T) or FALSE (F), and the logical connectives $\wedge$, $\vee$, and $\neg$ (and others discussed subsequently). Such an expression $P(p, q, \ldots)$ will be called a *proposition*.

The main property of a proposition $P(p, q, \ldots)$ is that its truth value depends exclusively upon the truth values of its variables, that is, the truth value of a proposition is known once the truth value of each of its variables is known. A simple concise way to show this relationship is through a *truth table*. We describe a way to obtain such a truth table below.

Consider, for example, the proposition $\neg\,(p \wedge \neg\, q)$. Figure 4-2(*a*) indicates how the truth table of $\neg\,(p \wedge \neg\, q)$ is constructed. Observe that the first columns of the table are for the variables $p, q, \ldots$ and that there are enough rows in the table to allow for all possible combinations of T and F for these *variables*. (For 2 variables, as above, 4 rows are necessary; for 3 variables, 8 rows are necessary; and, in general, for n variables, 2^n rows are required.) There is then a column for each "elementary" stage of the construction of the proposition, the truth value at each step being determined from the previous stages by the definitions of the connectives $\wedge, \vee, \neg$. Finally we obtain the truth value of the proposition, which appears in the last column.

The actual truth table of the proposition $\neg\,(p \wedge \neg\, q)$ is shown in Fig. 4-2(*b*). It consists precisely of the columns in Fig. 4-2(*a*) which appear under the variables and under the proposition; the other columns were merely used in the construction of the truth table.

p	q	$\neg\, q$	$p \wedge \neg\, q$	$\neg(p \wedge \neg\, q)$
T	T	F	F	T
T	F	T	T	F
F	T	F	F	T
F	F	T	F	T

(*a*)

p	q	$\neg(p \wedge \neg\, q)$
T	T	T
T	F	F
F	T	T
F	F	T

(*b*)

Fig. 4-2

Remark: In order to avoid an excessive number of parentheses, we sometimes adopt an order of precedence for the logical connectives. Specifically,

$$\neg \text{ has precedence over } \wedge \text{ which has precedence over } \vee$$

For example, $\neg\, p \wedge q$ means $(\neg\, p) \wedge q$ and not $\neg\,(p \wedge q)$.

Alternative Method for Constructing a Truth Table

Another way to construct the truth table for $\neg\,(p \wedge \neg\, q)$ follows:

(*a*) First we construct the truth table shown in Fig. 4-3. That is, first we list all the variables and the combinations of their truth values. Then the proposition is written on the top row to the right of its variables with sufficient space so that there is a column under each variable and each connective in the proposition. Also there is a final row labeled "Step".

p	q	$\neg$	$(p$	$\wedge$	$\neg$	$q)$
T	T					
T	F					
F	T					
F	F					
Step						

Fig. 4-3

(*b*) Next, additional truth values are entered into the truth table in various steps as shown in Fig. 4-4. That is, first the truth values of the variables are entered under the variables in the proposition, and then there is a column of truth values entered under each logical operation. We also indicate the step in which each column of truth values is entered in the table.

The truth table of the proposition then consists of the original columns under the variables and the last step, that is, the last column entered into the table.

p	q	$\neg$	$(p$	$\wedge$	$\neg$	$q)$
T	T		T			T
T	F		T			F
F	T		F			T
F	F		F			F
Step			1			1

(*a*)

p	q	$\neg$	$(p$	$\wedge$	$\neg$	$q)$
T	T		T		F	T
T	F		T		T	F
F	T		F		F	T
F	F		F		T	F
Step			1		2	1

(*b*)

p	q	$\neg$	$(p$	$\wedge$	$\neg$	$q)$
T	T		T	F	F	T
T	F		T	T	T	F
F	T		F	F	F	T
F	F		F	F	T	F
Step			1	3	2	1

(*c*)

p	q	$\neg$	$(p$	$\wedge$	$\neg$	$q)$
T	T	T	T	F	F	T
F	T	F	T	T	T	F
F	F	T	F	F	F	T
F	F	T	F	F	T	F
Step		4	1	3	2	1

(*d*)

Fig. 4-4

4.5 TAUTOLOGIES AND CONTRADICTIONS

Some propositions $P(p, q, \ldots)$ contain only T in the last column of their truth tables or, in other words, they are true for any truth values of their variables. Such propositions are called *tautologies*. Analogously, a proposition $P(p, q, \ldots)$ is called a *contradiction* if it contains only F in the last column of its truth table or, in other words, if it is false for any truth values of its variables. For example, the proposition "p or not p", that is, $p \vee \neg p$, is a tautology, and the proposition "p and not p", that is, $p \wedge \neg p$, is a contradiction. This is verified by looking at their truth tables in Fig. 4-5. (The truth tables have only two rows since each proposition has only the one variable p.)

p	$\neg p$	$p \vee \neg p$
T	F	T
F	T	T

(*a*) $p \vee \neg p$

p	$\neg p$	$p \wedge \neg p$
T	F	F
F	T	F

(*b*) $p \wedge \neg p$

Fig. 4-5

Note that the negation of a tautology is a contradiction since it is always false, and the negation of a contradiction is a tautology since it is always true.

Now let $P(p, q, \ldots)$ be a tautology, and let $P_1(p, q, \ldots), P_2(p, q, \ldots), \ldots$ be any propositions. Since $P(p, q, \ldots)$ does not depend upon the particular truth values of its variables $p, q, \ldots$, we can substitute P_1 for p, P_2 for $q, \ldots$ in the tautology $P(p, q, \ldots)$ and still have a tautology. In other words:

Theorem 4.1 (Principle of Substitution): If $P(p, q, \ldots)$ is a tautology, then $P(P_1, P_2, \ldots)$ is a tautology for any propositions $P_1, P_2, \ldots$.

4.6 LOGICAL EQUIVALENCE

Two propositions $P(p, q, \ldots)$ and $Q(p, q, \ldots)$ are said to be *logically equivalent*, or simply *equivalent* or *equal*, denoted by

$$P(p, q, \ldots) \equiv Q(p, q, \ldots)$$

if they have identical truth tables. Consider, for example, the truth tables of $\neg (p \wedge q)$ and $\neg p \vee \neg q$ appearing in Fig. 4-6. Observe that both truth tables are the same, that is, both propositions are false in the first case and true in the other three cases. Accordingly, we can write

$$\neg (p \wedge q) \equiv \neg p \vee \neg q$$

In other words, the propositions are logically equivalent.

Remark: Consider the statement

"It is not the case that roses are red and violets are blue"

This statement can be written in the form $\neg (p \vee q)$ where:

p is "roses are red" and q is "violets are blue"

However, as noted above, $\neg (p \wedge q) \equiv \neg p \vee \neg q$. Thus the statement

"Roses are not red, or violets are not Blue."

has the same meaning as the given statement.

p	q	$p \wedge q$	$\neg (p \wedge q)$
T	T	T	F
T	F	F	T
F	T	F	T
F	F	F	T

(*a*) $\neg (p \wedge q)$

p	q	$\neg p$	$\neg q$	$\neg p \vee \neg q$
T	T	F	F	F
T	F	F	T	T
F	T	T	F	T
F	F	T	T	T

(*b*) $\neg p \vee \neg q$

Fig. 4-6

4.7 ALGEBRA OF PROPOSITIONS

Propositions satisfy various laws which are listed in Table 4-1. (In this table, T and F are restricted to the truth values "true" and "false", respectively.) We state this result formally.

Theorem 4.2: Propositions satisfy the laws of Table 4-1.

Table 4-1 Laws of the algebra of propositions

Idempotent laws	
(1*a*) $p \vee p \equiv p$	(1*b*) $p \wedge p \equiv p$
Associative laws	
(2*a*) $(p \vee q) \vee r \equiv p \vee (q \vee r)$	(2*b*) $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$
Commutative laws	
(3*a*) $p \vee q \equiv q \vee p$	(3*b*) $p \wedge q \equiv q \wedge p$
Distributive laws	
(4*a*) $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$	(4*b*) $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$
Identity laws	
(5*a*) $p \vee \mathrm{F} \equiv p$	(5*b*) $p \wedge \mathrm{T} \equiv p$
(6*a*) $p \vee \mathrm{T} \equiv \mathrm{T}$	(6*b*) $p \wedge \mathrm{F} \equiv \mathrm{F}$
Complement laws	
(7*a*) $p \vee \neg p \equiv \mathrm{T}$	(7*b*) $p \wedge \neg p \equiv \mathrm{F}$
(8*a*) $\neg\mathrm{T} \equiv \mathrm{F}$	(8*b*) $\neg\mathrm{F} \equiv \mathrm{T}$
Involution law	
(9) $\neg\neg p \equiv p$	
DeMorgan's laws	
(10*a*) $\neg(p \vee q) \equiv \neg p \wedge \neg q$	(10*b*) $\neg(p \wedge q) \equiv \neg p \vee \neg q$

4.8 CONDITIONAL AND BICONDITIONAL STATEMENTS

Many statements, particularly in mathematics, are of the form "If p then q". Such statements are called *conditional* statements and are denoted by

$$p \rightarrow q$$

The conditional $p \rightarrow q$ is frequently read "p implies q" or "p only if q".

Another common statement is of the form "p if and only if q". Such statements are called *biconditional* statements and are denoted by

$$p \leftrightarrow q$$

p	q	$p \rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

(*a*) $p \rightarrow q$

p	q	$p \leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

(*b*) $p \leftrightarrow q$

Fig. 4-7

p	q	$\neg p$	$\neg p \vee q$
T	T	F	T
T	F	F	F
F	T	T	T
F	F	T	T

$\neg p \vee q$

Fig. 4-8

The truth values of $p \to q$ and $p \leftrightarrow q$ are defined by the tables in Fig. 4-7. Observe that:

(*a*) The conditional $p \to q$ is false only when the first part p is true and the second part q is false. Accordingly, when p is false, the conditional $p \to q$ is true regardless of the truth value of q.

(*b*) The biconditional $p \leftrightarrow q$ is true whenever p and q have the same truth values and false otherwise.

The truth table of the proposition $\neg p \vee q$ appears in Fig. 4-8. Observe that the truth tables of $\neg p \vee q$ and $p \to q$ are identical, that is, they are both false only in the second case. Accordingly, $p \to q$ is logically equivalent to $\neg p \vee q$; that is,

$$p \to q \equiv \neg p \vee q$$

In other words, the conditional statement "If p then q" is logically equivalent to the statement "Not p or q" which only involves the connectives $\vee$ and $\neg$ and thus was already a part of our language. We may regard $p \to q$ as an abbreviation for an oft-recurring statement.

4.9 ARGUMENTS

An *argument* is an assertion that a given set of propositions $P_1, P_2, \ldots, P_n$, called *premises*, yields (has a consequence) another proposition Q, called the *conclusion*. Such an argument is denoted by

$$P_1, P_2, \ldots, P_n \vdash Q$$

The notion of a "logical argument" or "valid argument" is formalized as follows:

Definition 4.4: An argument $P_1, P_2, \ldots, P_n \vdash Q$ is said to be *valid* if Q is true whenever all the premises $P_1, P_2, \ldots, P_n$ are true.

An argument which is not valid is called a *fallacy*.

EXAMPLE 4.5

(*a*) The following argument is valid:

$$p, p \to q \vdash q \qquad (\textbf{\textit{Law of Detachment}})$$

The proof of this rule follows from the truth table in Fig. 4-9. Specifically, p and $p \to q$ are true simultaneously only in Case (row) 1, and in this case q is true.

(*b*) The following argument is a fallacy:

$$p \to q, q \vdash p$$

For $p \to q$ and q are both true in Case (row) 3 in the truth table in Fig. 4-9, but in this case p is false.

p	q	$p \to q$
T	T	T
T	F	F
F	T	T
F	F	T

Fig. 4-9

Now the propositions $P_1, P_2, \ldots, P_n$ are true simultaneously if and only if the proposition $P_1 \wedge P_2 \wedge \ldots \wedge P_n$ is true. Thus the argument $P_1, P_2, \ldots, P_n \vdash Q$ is valid if and only if Q is true whenever $P_1 \wedge P_2 \wedge \ldots \wedge P_n$ is true or, equivalently, if the proposition $(P_1 \wedge P_2 \wedge \ldots \wedge P_n) \to Q$ is a tautology. We state this result formally.

Theorem 4.3: The argument $P_1, P_2, \ldots, P_n \vdash Q$ is valid if and only if the proposition $(P_1 \wedge P_2 \ldots \wedge P_n) \rightarrow Q$ is a tautology.

We apply this theorem in the next example.

EXAMPLE 4.6 A fundamental principle of logical reasoning states:

"If p implies q and q implies r, then p implies r."

That is, the following argument is valid:

$$p \rightarrow q,\ q \rightarrow r \vdash p \rightarrow r \ (\textbf{\textit{Law of Syllogism}})$$

This fact is verified by the truth table in Fig. 4-10 which shows that the following proposition is a tautology:

$$[(p \rightarrow q) \wedge (q \rightarrow r)] \rightarrow (p \rightarrow r)$$

Equivalently, the argument is valid since the premises $p \rightarrow q$ and $q \rightarrow r$ are true simultaneously only in Cases (rows) 1, 5, 7 and 8, and in these cases the conclusion $p \rightarrow r$ is also true. (Observe that the truth table required $2^3 = 8$ lines since there are three variables p, q and r.)

p	q	r	$[(p$	$\rightarrow$	$q)$	$\wedge$	$(q$	$\rightarrow$	$r)]$	$\rightarrow$	$(p$	$\rightarrow$	$r)$
T	T	T	T	T	T	T	T	T	T	T	T	T	T
T	T	F	T	T	T	F	T	F	F	T	T	F	F
T	F	T	T	F	F	F	F	T	T	T	T	T	T
T	F	F	T	F	F	F	F	T	F	T	T	F	F
F	T	T	F	T	T	T	T	T	T	T	F	T	T
F	T	F	F	T	T	F	T	F	F	T	F	T	F
F	F	T	F	T	F	T	F	T	T	T	F	T	T
F	F	F	F	T	F	T	F	T	F	T	F	T	F
Step			1	2	1	3	1	2	1	4	1	2	1

Fig. 4-10

We now apply the above theory to arguments involving specific statements. We emphasize that the validity of an argument does not depend upon the truth values nor the content of the statements appearing in the argument, but upon the particular form of the argument. This is illustrated in the following example.

EXAMPLE 4.7 Consider the following argument:

S_1: If a man is a bachelor, he is unhappy.
S_2: If a man is unhappy, he dies young.
.....
S: Bachelors die young.

Here the statement S below the line denotes the conclusion of the argument, and the statements S_1 and S_2 above the line denote the premises. We claim that the argument $S_1, S_2 \vdash S$ is valid. For the argument is of the form

$$p \rightarrow q, q \rightarrow r \vdash p \rightarrow r$$

where p is "He is a bachelor", q is "He is unhappy" and r is "He dies young"; and by Example 4.6 this argument (Law of Syllogism) is valid.

4.10 LOGICAL IMPLICATION

A proposition $P(p, q, \ldots)$ is said to *logically imply* a proposition $Q(p, q, \ldots)$, written

$$P(p, q, \ldots) \Rightarrow Q(p, q, \ldots)$$

if $Q(p, q, \ldots)$ is true whenever $P(p, q, \ldots)$ is true.

EXAMPLE 4.8 We claim that p logically implies $p \vee q$. For consider the truth table in Fig. 4-11. Observe that p is true in Cases (rows) 1 and 2, and in these cases $p \vee q$ is also true. Thus $p \Rightarrow p \vee q$.

p	q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

Fig. 4-11

Now if $Q(p, q, \ldots)$ is true whenever $P(p, q, \ldots)$ is true, then the argument

$$P(p, q, \ldots) \vdash Q(p, q, \ldots)$$

is valid; and conversely. Furthermore, the argument $P \vdash Q$ is valid if and only if the conditional statement $P \rightarrow Q$ is always true, i.e., a tautology. We state this result formally.

Theorem 4.4: For any propositions $P(p, q, \ldots)$ and $Q(p, q, \ldots)$, the following three statements are equivalent:

(i) $P(p, q, \ldots)$ logically implies $Q(p, q, \ldots)$.

(ii) The argument $P(p, q, \ldots) \vdash Q(p, q, \ldots)$ is valid.

(iii) The proposition $P(p, q, \ldots) \rightarrow Q(p, q, \ldots)$ is a tautology.

We note that some logicians and many texts use the word "implies" in the same sense as we use "logically implies", and so they distinguish between "implies" and "if... then". These two distinct concepts are, of course, intimately related as seen in the above theorem.

4.11 PROPOSITIONAL FUNCTIONS, QUANTIFIERS

Let A be a given set. A *propositional function* (or: an *open sentence* or *condition*) defined on A is an expression

$$p(x)$$

which has the property that $p(a)$ is true or false for each $a \in A$. That is, $p(x)$ becomes a statement (with a truth value) whenever any element $a \in A$ is substituted for the variable x. The set A is called the *domain* of $p(x)$, and the set T_p of all elements of A for which $p(a)$ is true is called the *truth set* of $p(x)$. In other words,

$$T_p = \{x\colon x \in A,\ p(x) \text{ is true}\} \qquad \text{or} \qquad T_p = \{x\colon p(x)\}$$

Frequently, when A is some set of numbers, the condition $p(x)$ has the form of an equation or inequality involving the variable x.

EXAMPLE 4.9 Find the truth set of each propositional function $p(x)$ defined on the set $\mathbf{N}$ of positive integers.

(*a*) Let $p(x)$ be "$x + 2 > 7$". Its truth set is

$$\{x: x \in \mathbf{N},\ x + 2 > 7\} = \{6, 7, 8, \ldots\}$$

consisting of all integers greater than 5.

(*b*) Let $p(x)$ be "$x + 5 < 3$". Its truth set is

$$\{x: x \in \mathbf{N},\ x + 5 < 3\} = \varnothing$$

the empty set. In other words, $p(x)$ is not true for any positive integer in $\mathbf{N}$.

(*c*) Let $p(x)$ be "$x + 5 > 1$". Its truth set is

$$\{x: x \in \mathbf{N},\ x + 5 > 1\} = \mathbf{N}$$

Thus $p(x)$ is true for every element in $\mathbf{N}$.

Remark: The above example shows that if $p(x)$ is a propositional function defined on a set A then $p(x)$ could be true for all $x \in A$, for some $x \in A$, or for no $x \in A$. The next two subsections discusses quantifiers related to such propositional functions.

Universal Quantifier

Let $p(x)$ be a propositional function defined on a set A. Consider the expression

$$(\forall x \in A)p(x) \qquad \text{or} \qquad \forall x\ p(x) \tag{4.1}$$

which reads "For every x in A, $p(x)$ is a true statement" or, simply, "For all x, $p(x)$". The symbol

$$\forall$$

which reads "for all" or "for every" is called the *universal quantifier*. The statement (*4.1*) is equivalent to the statement

$$T_p = \{x: x \in A,\ p(x)\} = A \tag{4.2}$$

that is, that the truth set of $p(x)$ is the entire set A.

The expression $p(x)$ by itself is an open sentence or condition and therefore has no truth value. However, $\forall x\ p(x)$, that is $p(x)$ preceded by the quantifier $\forall$, does have a truth value which follows from the equivalence of (*4.1*) and (*4.2*). Specifically:

Q_1: If $\{x: x \in A, p(x)\} = A$ then $\forall x\ p(x)$ is true; otherwise, $\forall x\ p(x)$ is false.

EXAMPLE 4.10

(*a*) The proposition $(\forall n \in \mathbf{N})(n + 4 > 3)$ is true since

$$\{n: n + 4 > 3\} = \{1, 2, 3, \ldots\} = \mathbf{N}$$

(*b*) The proposition $(\forall n \in \mathbf{N})(n + 2 > 8)$ is false since

$$\{n: n + 2 > 8\} = \{7, 8, \ldots\} \neq \mathbf{N}$$

(*c*) The symbol $\forall$ can be used to define the intersection of an indexed collection $\{A_i: i \in I\}$ of sets A_i as follows:

$$\cap(A_i: i \in I) = \{x: \forall_i \in I,\ x \in A_i\}$$

Existential Quantifier

Let $p(x)$ be a propositional function defined on a set A. Consider the expression

$$(\exists x \in A)p(x) \qquad \text{or} \qquad \exists x,\ p(x) \tag{4.3}$$

which reads "There exists an x in A such that $p(x)$ is a true statement" or, simply, "For some x, $p(x)$". The symbol

$$\exists$$

which reads "there exists" or "for some" or "for at least one" is called the *existential quantifier*. Statement (*4.3*) is equivalent to the statement

$$T_p = \{x\colon x \in A,\ p(x)\} \neq \varnothing \tag{4.4}$$

i.e., that the truth set of $p(x)$ is not empty. Accordingly, $\exists x\, p(x)$, that is, $p(x)$ preceded by the quantifier $\exists$, does have a truth value. Specifically:

Q_2: If $\{x\colon p(x)\} \neq \varnothing$ then $\exists\, x\ p(x)$ is true; otherwise, $\exists x\, p(x)$ is false.

EXAMPLE 4.11

(*a*) The proposition $(\exists\, n \in \mathbf{N})(n + 4 < 7)$ is true since $\{n\colon n + 4 < 7\} = \{1, 2\} \neq \varnothing$.

(*b*) The proposition $(\exists\, n \in \mathbf{N})(n + 6 < 4)$ is false since $(n\colon n + 6 < 4\} = \varnothing$.

(*c*) The symbol $\exists$ can be used to define the union of an indexed collection $\{A_i\colon i \in I\}$ of sets A_i as follows:

$$\cup(A_i\colon i \in I) = \{x\colon \exists\, i \in I,\ x \in A_i\}$$

Notation

Let $A = \{2, 3, 5\}$ and let $p(x)$ be the sentence "x is a prime number" or, simply "x is prime". Then

"Two is prime and three is prime and five is prime" $\qquad (*)$

can be denoted by

$$p(2) \wedge p(3) \wedge p(5) \qquad \text{or} \qquad \wedge\,(a \in A,\ p(a))$$

which is equivalent to the statement

"Every number in A is prime" $\qquad$ or $\qquad \forall a \in A,\ p(a) \qquad (**)$

Similarly, the proposition

"Two is prime or three is prime or five is prime."

can be denoted by

$$p(2) \vee p(3) \vee p(5) \qquad \text{or} \qquad \vee\,(a \in A,\ p(a))$$

which is equivalent to the statement

"At least one number in A is prime" $\qquad$ or $\qquad \exists\, a \in A,\ p(a)$

In other words

$$\wedge(a \in A,\ p(a)) \equiv \forall a \in A,\ p(a) \qquad \text{and} \qquad \vee\,(a \in A,\ p(a)) \equiv \exists a \in A,\ p(a)$$

Thus the symbols $\wedge$ and $\vee$ are sometimes used instead of $\forall$ and $\exists$.

Remark: If A were an infinite set, then a statement of the form $(*)$ cannot be made since the sentence would not end; but a statement of the form $(**)$ can always be made, even when A is infinite.

4.12 NEGATION OF QUANTIFIED STATEMENTS

Consider the statement: "All math majors are male". Its negation reads:

"It is not the case that all math majors are male" or, equivalently,

"There exists at least one math major who is a female (not male)"

Symbolically, using M to denoted the set of math majors, the above can be written as

$$\neg(\forall x \in M)\,(x \text{ is male}) \equiv (\exists\, x \in M)\ (x \text{ is not male})$$

or, when $p(x)$ denotes "x is male",

$$\neg(\forall x \in M)p(x) \equiv (\exists\, x \in M)\neg\, p(x) \qquad \text{or} \qquad \neg\forall x p(x) \equiv \exists\, x \neg\, p(x)$$

The above is true for any proposition p(x). That is:

Theorem 4.5 (DeMorgan): $\neg\,(\forall x \in A)p(x) \equiv (\exists\, x \in A)\neg\, p(x)$.

In other words, the following two statements are equivalent:

(1) It is not true that, for all $a \in A$, $p(a)$ is true.
(2) There exists an $a \in A$ such that $p(a)$ is false.

There is an analogous theorem for the negation of a proposition which contains the existential quantifier.

Theorem 4.6 (DeMorgan): $\neg\,(\exists x \in A)p(x) \equiv (\forall x \in A)\neg\, p(x)$.

That is, the following two statements are equivalent:

(1) It is not true that for some $a \in A$, $p(a)$ is true.
(2) For all $a \in A$, $p(a)$ is false.

EXAMPLE 4.12

(*a*) The following statements are negatives of each other:

"For all positive integers n we have $n + 2 > 8$"

"There exists a positive integer n such that $n + 2 \not> 8$"

(*b*) The following statements are also negatives of each other:

"There exists a (living) person who is 150 years old"

"Every living person is not 150 years old"

Remark: The expression $\neg\, p(x)$ has the obvious meaning; that is:

"The statement $\neg\, p(a)$ is true when $p(a)$ is false, and vice versa"

Previously, $\neg$ was used as an operation on statements; here $\neg$ is used as an operation on propositional functions. Similarly, $p(x) \wedge q(x)$, read "$p(x)$ and $q(x)$", is defined by:

"The statement $p(a) \wedge q(a)$ is true when $p(a)$ and $q(a)$ are true"

Similarly, $p(x) \vee q(x)$, read "$p(x)$ or $q(x)$", is defined by:

"The statement $p(a) \vee q(a)$ is true when $p(a)$ or $q(a)$ is true"

Thus in terms of truth sets:

(i) $\neg\, p(x)$ is the complement of $p(x)$.
(ii) $p(x) \wedge q(x)$ is the intersection of $p(x)$ and $q(x)$.
(iii) $p(x) \vee q(x)$ is the union of $p(x)$ and $q(x)$.

One can also show that the laws for propositions also hold for propositional functions. For example, we have DeMorgan's laws;

$$\neg\,(p(x) \wedge q(x)) \equiv \neg\, p(x) \vee \neg\, q(x) \qquad \text{and} \qquad \neg\,(p(x) \vee q(x)) \equiv \neg\, p(x) \wedge \neg\, q(x)$$

Counterexample

Theorem 4.6 tells us that to show that a statement $\forall x, p(x)$ is false, it is equivalent to show that $\exists\, x \neg\, p(x)$ is true or, in other words, that there is an element x_0 with the property that $p(x_0)$ is false. Such an element x_0 is called a *counterexample* to the statement $\forall x, p(x)$.

EXAMPLE 4.13

(*a*) Consider the statement $\forall x \in \mathbf{R}, |x| \neq 0$. The statement is false since 0 is a counterexample, that is, $|0| \neq 0$ is not true.

(*b*) Consider the statement $\forall x \in \mathbf{R}$, $x^2 \geq x$. The statement is not true since, for example, $\frac{1}{2}$ is a counterexample. Specifically, $(\frac{1}{2})^2 \geq \frac{1}{2}$ is not true, that is, $(\frac{1}{2})^2 < \frac{1}{2}$.

(*c*) Consider the statement $\forall x \in \mathbf{N}$, $x^2 \geq x$. This statement is true where $\mathbf{N}$ is the set of positive integers. In other words, there does not exist a positive integer n for which $n^2 < n$.

Propositional Functions with More Than One Variable

A propositional function (of n variables) defined over a product set $A = A_1 \times \ldots \times A_n$ is an expression

$$p(x_1, x_2, \ldots, x_n)$$

which has the property that $p(a_1, a_2, \ldots, a_n)$ is true or false for any n-tuple $(a_1, \ldots a_n)$ in A. For example,

$$x + 2y + 3z < 18$$

is a propositional function on $\mathbf{N}^3 = \mathbf{N} \times \mathbf{N} \times \mathbf{N}$. Such a propositional function has no truth value. However, we do have the following:

Basic Principle: A propositional function preceded by a quantifier for each variable, for example,

$$\forall x\, \exists y,\, p(x, y) \qquad \text{or} \qquad \exists x\, \forall y\, \exists\, z,\, p(x, y, z)$$

denotes a statement and has a truth value.

EXAMPLE 4.14 Let $B = \{1, 2, 3, \ldots, 9\}$ and let $p(x, y)$ denote "$x + y = 10$". Then $p(x, y)$ is a propositional function on $A = B^2 = B \times B$.

(*a*) The following is a statement since there is a quantifier for each variable:

$$\forall x\, \exists\, y,\, p(x, y), \qquad \text{that is,} \qquad \text{"For every } x\text{, there exists a } y \text{ such that } x + y = 10\text{"}$$

This statement is true. For example, if $x = 1$, let $y = 9$; if $x = 2$, let $y = 8$, and so on.

(*b*) The following is also a statement:

$$\exists\, y\, \forall x,\, p(x, y), \text{ that is, "There exists a } y \text{ such that, for every } x\text{, we have } x + y = 10\text{"}$$

No such y exists; hence this statement is false.

Note that the only difference between (*a*) and (*b*) is the order of the quantifiers. Thus a different ordering of the quantifiers may yield a different statement. We note that, when translating such quantified statements into English, the expression "such that" frequently follows "there exists".

Negating Quantified Statements with More Than One Variable

Quantified statements with more than one variable may be negated by successively applying Theorems 4.5 and 4.6. Thus each $\forall$ is changed to $\exists$ and each $\exists$ is changed to $\forall$ as the negation symbol $\neg$ passes through the statement from left to right. For example,

$$\begin{aligned}\neg[\forall x \exists y \exists z, p(x, y, z)] &\equiv \exists x \neg[\exists y \exists z, p(x, y, z)] \equiv \exists x \forall y[\neg \exists z, p(x, y, z) \\ &\equiv \exists x \, \forall y \, \forall z, \, \neg p(x, y, z)\end{aligned}$$

Naturally, we do not put in all the steps when negating such quantified statements.

EXAMPLE 4.15

(*a*) Consider the quantified statement:

"Every student has at least one course where the lecturer is a teaching assistant"

Its negation is the statement:

"There is a student such that in every course the lecturer is not a teaching assistant"

(*b*) The formal definition that L is the limit of a sequence $a_1, a_2, \ldots$ follows:

$$\forall \in > 0, \exists \, n_0 \in \mathbf{N}, \quad \forall n > n_0, \quad |a_n - L| < \in$$

Thus L is not the limit of the sequence $a_1, a_2, \ldots$ when:

$$\exists \in > 0, \quad \forall \, n_0 \in \mathbf{N}, \quad \exists n > n_0, \quad |a_n - L| \geq \in$$

Solved Problems

PROPOSITIONS AND LOGICAL OPERATIONS

4.1. Let p be "It is cold" and let q be "It is raining". Give a simple verbal sentence which describes each of the following statements: (*a*) $\neg p$; (*b*) $p \wedge q$; (*c*) $p \vee q$; (*d*) $q \vee \neg p$.

In each case, translate $\wedge$, $\vee$, and $\sim$ to read "and", "or", and "It is false that" or "not", respectively, and then simplify the English sentence.

(*a*) It is not cold.

(*b*) It is cold and raining.

(*c*) It is cold or it is raining.

(*d*) It is raining or it is not cold.

4.2. Let p be "Erik reads *Newsweek*", let q be "Erik reads *The New Yorker*", and let r be "Erik reads *Time*". Write each of the following in symbolic form:

(*a*) Erik reads *Newsweek* or *The New Yorker*, but not *Time*.

(*b*) Erik reads *Newsweek* and *The New Yorker*, or he does not read *Newsweek* and *Time*.

(*c*) It is not true that Erik reads *Newsweek* but not *Time*.

(*d*) It is not true that Erik reads *Time* or *The New Yorker* but not *Newsweek*.

Use $\vee$ for "or", $\wedge$ for "and" (or, its logical equivalent, "but"), and $\neg$ for "not" (negation).

(*a*) $(p \vee q) \wedge \neg r$; (*b*) $(p \wedge q) \vee \neg (p \wedge r)$; (*c*) $\neg (p \wedge \neg r)$; (*d*) $\neg [(r \vee q) \wedge \neg p]$.

TRUTH VALUES AND TRUTH TABLES

4.3. Determine the truth value of each of the following statements:

(*a*) $4 + 2 = 5$ and $6 + 3 = 9$.
(*b*) $3 + 2 = 5$ and $6 + 1 = 7$.
(*c*) $4 + 5 = 9$ and $1 + 2 = 4$.
(*d*) $3 + 2 = 5$ and $4 + 7 = 11$.

The statement "p and q" is true only when both substatements are true. Thus: (*a*) false; (*b*) true; (*c*) false; (*d*) true.

4.4. Find the truth table of $\neg p \wedge q$.

See Fig. 4-12, which gives both methods for constructing the truth table.

p	q	$\neg p$	$\neg p \wedge q$
T	T	F	F
T	F	F	F
F	T	T	T
F	F	T	F

(*a*) Method 1

p	q	$\neg$	p	$\wedge$	q
T	T	F	T	F	T
T	F	F	T	F	F
F	T	T	F	T	T
F	F	T	F	F	F
		Step 2	1	3	1

(*b*) Method 2

Fig. 4-12

4.5. Verify that the proposition $p \vee \neg (p \wedge q)$ is tautology.

Construct the truth table of $p \vee \neg (p \wedge q)$ as shown in Fig. 4-13. Since the truth value of $p \vee \neg (p \wedge q)$ is T for all values of p and q, the proposition is a tautology.

p	q	$p \wedge q$	$\neg (p \wedge q)$	$p \vee \neg (p \wedge q)$
T	T	T	F	T
T	F	F	T	T
F	T	F	T	T
F	F	F	T	T

Fig. 4-13

4.6. Show that the propositions $\neg (p \wedge q)$ and $\neg p \vee \neg q$ are logically equivalent.

Construct the truth tables for $\neg (p \wedge q)$ and $\neg p \vee \neg q$ as in Fig. 4-14. Since the truth tables are the same (both propositions are false in the first case and true in the other three cases), the propositions $\neg (p \wedge q)$ and $\neg p \vee \neg q$ are logically equivalent and we can write

$$\neg (p \wedge q) \equiv \neg p \vee \neg q$$

p	q	$p \wedge q$	$\neg (p \wedge q)$
T	T	T	F
T	F	F	T
F	T	F	T
F	F	F	T

(*a*) $\neg (p \wedge q)$

p	q	$\neg p$	$\neg q$	$\neg p \vee \neg q$
T	T	F	F	F
T	F	F	T	T
F	T	T	F	T
F	F	T	T	T

(*b*) $\neg p \vee \neg q$

Fig. 4-14

4.7. Use the laws in Table 4-1 to show that $\neg (p \vee q) \vee (\neg p \wedge q) \equiv \neg p$.

	Statement	Reason
(1)	$\neg (p \vee q) \vee (\neg p \wedge q) \equiv (\neg p \wedge \neg q) \vee (\neg p \wedge q)$	DeMorgan's law
(2)	$\equiv \neg p \wedge (\neg q \vee q)$	Distributive law
(3)	$\equiv \neg p \wedge T$	Complement law
(4)	$\equiv \neg p$	Identity law

CONDITIONAL STATEMENTS

4.8. Rewrite the following statements without using the conditional:

(*a*) If it is cold, he wears a hat.

(*b*) If productivity increases, then wages rise.

Recall that "If p then q" is equivalent to "Not p or q"; that is, $p \rightarrow q \equiv \neg p \vee q$. Hence,

(*a*) It is not cold or he wears a hat.

(*b*) Productivity does not increase or wages rise.

4.9. Determine the contrapositive of each statement:

(*a*) If John is a poet, then he is poor;

(*b*) Only if Marc studies will he pass the test.

(*a*) The contrapositive of $p \rightarrow q$ is $\neg q \rightarrow \neg p$. Hence the contrapositive of the given statement is

If John is not poor, then he is not a poet.

(*b*) The given statement is equivalent to "If Marc passes the test, then he studied". Hence its contrapositive is

If Marc does not study, then he will not pass the test.

4.10. Consider the conditional proposition $p \rightarrow q$. The simple propositions $q \rightarrow p$, $\neg p \rightarrow \neg q$, and $\neg q \rightarrow \neg p$ are called, respectively, the *converse*, *inverse*, and *contrapositive* of the conditional $p \rightarrow q$. Which if any of these propositions are logically equivalent to $p \rightarrow q$?

Construct their truth tables as in Fig. 4-15. Only the contrapositive $\neg q \rightarrow \neg p$ is logically equivalent to the original conditional proposition $p \rightarrow q$.

p	q	$\neg p$	$\neg q$	Conditional $p \rightarrow q$	Converse $q \rightarrow p$	Inverse $\neg p \rightarrow \neg q$	Contrapositive $\neg q \rightarrow \neg p$
T	T	F	F	T	T	T	T
T	F	F	T	F	T	T	F
F	T	T	F	T	F	F	T
F	F	T	T	T	T	T	T

Fig. 4-15

4.11. Write the negation of each statement as simply as possible:

(*a*) If she works, she will earn money.

(*b*) He swims if and only if the water is warm.

(*c*) If it snows, then they do not drive the car.

(*a*) Note that $\neg (p \rightarrow q) \equiv p \wedge \neg q$; hence the negation of the statement follows:

She works or she will not earn money.

(*b*) Note that $\neg (p \leftrightarrow q) \equiv p \leftrightarrow \neg q \equiv \neg p \leftrightarrow q$; hence the negation of the statement is either of the following:

He swims if and only if the water is not warm.
He does not swim if and only if the water is warm.

(*c*) Note that $\neg (p \rightarrow \neg q) \equiv p \wedge \neg \neg q \equiv p \wedge q$. Hence the negation of the statement follows:

It snows and they drive the car.

ARGUMENTS

4.12. Show that the following argument is a fallacy: $p \rightarrow q$, $\neg p \vdash \neg q$.

Construct the truth table for $[(p \rightarrow q) \wedge \neg p] \rightarrow \neg q$ as in Fig. 4-16. Since the proposition $[(p \rightarrow q) \wedge \neg p] \rightarrow \neg q$ is not a tautology, the argument is a fallacy. Equivalently, the argument is a fallacy since in third line of the truth table $p \rightarrow q$ and $\neg p$ are true but $\neg q$ is false.

p	q	$p \rightarrow q$	$\neg p$	$(p \rightarrow q) \wedge \neg p$	$\neg q$	$[(p \rightarrow q) \wedge \neg p] \rightarrow \neg q$
T	T	T	F	F	F	T
T	F	F	F	F	T	T
F	T	T	T	T	F	F
F	F	T	T	T	T	T

Fig. 4-16

4.13. Determine the validity of the following argument: $p \rightarrow q$, $\neg q \vdash \neg p$.

Construct the truth table for $[(p \rightarrow q) \wedge \neg q] \rightarrow \neg p$ as in Fig. 4-17. Since the proposition $[(p \rightarrow q) \wedge \neg q] \rightarrow \neg p$ is a tautology, the argument is valid.

p	q	$[(p$	$\rightarrow$	$q)$	$\wedge$	$\neg$	$q]$	$\rightarrow$	$\neg$	p
T	T	T	T	T	F	F	T	T	F	T
T	F	T	F	F	F	T	F	T	F	T
F	T	F	T	T	F	F	T	T	T	F
F	F	F	T	F	T	T	F	T	T	F
Step		1	2	1	3	2	1	4	2	1

Fig. 4-17

4.14. Prove that the following argument is valid: $p \to \neg q$, $r \to q$, $r \vdash \neg p$.

Construct the truth tables of the premises and conclusion as in Fig. 4-18. Now, $p \to \neg q$, $r \to q$, and r are true simultaneously only in the fifth row of the table, where $\neg p$ is also true. Hence, the argument is valid.

	p	q	r	$p \to \neg q$	$r \to q$	$\neg q$
1	T	T	T	F	T	F
2	T	T	F	F	T	F
3	T	F	T	T	F	F
4	T	F	F	T	T	F
5	F	T	T	T	T	T
6	F	T	F	T	T	T
7	F	F	T	T	F	T
8	F	F	F	T	T	T

Fig. 4-18

4.15. Test the validity of the following argument:

If two sides of a triangle are equal, then the opposite angles are equal.
Two sides of a triangle are not equal.

The opposite angles are not equal.

First translate the argument into the symbolic form $p \to q$, $\neg p \vdash \neg q$, where p is "Two sides of a triangle are equal" and q is "The opposite angles are equal". By Problem 4.12, this argument is a fallacy.

Remark: Although the conclusion *does* follow from the second premise and axioms of Euclidean geometry, the above argument does not constitute such a proof since the argument is a fallacy.

4.16. Determine the validity of the following argument:

If 7 is less than 4, then 7 is not a prime number.
7 is not less than 4.

---

7 is a prime number.

First translate the argument into symbolic form. Let p be "7 is less than 4" and q be "7 is a prime number". Then the argument is of the form

$$p \to \neg q,\ \neg p \vdash q$$

Now, we construct a truth table as shown in Fig. 4-19. The above argument is shown to be a fallacy since, in the fourth line of the truth table, the premises $p \to \neg q$ and $\neg p$ are true, but the conclusion q is false.

Remark: The fact that the conclusion of the argument happens to be a true statement is irrelevant to the fact that the argument presented is a fallacy.

p	q	$\neg q$	$p \to \neg q$	$\neg p$
T	T	F	F	F
T	F	T	T	F
F	T	F	T	T
F	F	T	T	T

Fig. 4-19

QUANTIFIERS AND PROPOSITIONAL FUNCTIONS

4.17. Let $A = \{1, 2, 3, 4, 5\}$. Determine the truth value of each of the following statements:

(*a*) $(\exists\, x \in A)(x + 3 = 10)$ (*b*) $(\forall x \in A)(x + 3 < 10)$

(*c*) $(\exists\, x \in A)(x + 3 < 5)$ (*d*) $(\forall x \in A)(x + 3 \leq 7)$

(*a*) False. For no number in A is a solution to $x + 3 = 10$.

(*b*) True. For every number in A satisfies $x + 3 < 10$.

(*c*) True. For if $x_0 = 1$, then $x_0 + 3 < 5$, i.e., 1 is a solution.

(*d*) False. For if $x_0 = 5$, then $x_0 + 3$ is not less than or equal 7. In other words, 5 is not a solution to the given condition.

4.18. Determine the truth value of each of the following statements where $\mathbf{U} = \{1, 2, 3\}$ is the universal set: (*a*) $\exists\, x\ \forall y, x^2 < y + 1$; (*b*) $\forall x\ \exists y, x^2 + y^2 < 12$; (*c*) $\forall x\ \forall y, x^2 + y^2 < 12$.

(*a*) True. For if $x = 1$, then 1, 2 and 3 are all solutions to $1 < y + 1$.

(*b*) True. For each x_0, let $y = 1$; then $x_0^2 + 1 < 12$ is a true statement.

(*c*) False. For if $x_0 = 2$ and $y_0 = 3$, then $x_0^2 + y_0^2 < 12$ is not a true statement.

4.19. Negate each of the following statements:

(*a*) $\exists x\ \forall y,\ p(x, y)$; (*b*) $\exists x \forall y,\ p(x, y)$; (*c*) $\exists y\ \exists x\ \forall z,\ p(x, y, z)$.

Use $\neg\, \forall x\, p(x) \equiv \exists x \neg\, p(x)$ and $\neg\, \exists x\, p(x) \equiv \forall x \neg\, p(x)$:

(*a*) $\neg\, (\exists x\ \forall y,\ p(x, y)) \equiv \forall x\ \exists y \neg\, p(x, y)$.

(*b*) $\neg\, (\forall x\ \forall y,\ p(x, y)) \equiv \exists x\ \exists y \neg\, p(x, y)$.

(*c*) $\neg\, (\exists y\ \exists x\ \forall z,\ p(x, y, z)) \equiv \forall y\ \forall x\ \exists z \neg\, p(x, y, z)$.

4.20. Let $p(x)$ denote the sentence "$x + 2 > 5$". State whether or not $p(x)$ is a propositional function on each of the following sets: (*a*) $\mathbf{N}$, the set of positive integers; (*b*) $M = \{-1, -2, -3, \ldots\}$; (*c*) $\mathbf{C}$, the set of complex number.

(*a*) Yes.

(*b*) Although $p(x)$ is false for every element in M, $p(x)$ is still a propositional function on M.

(*c*) No. Note that $2i + 2 > 5$ does not have any meaning. In other words, inequalities are not defined for complex numbers.

4.21. Negate each of the following statements: (*a*) All students live in the dormitories. (*b*) All mathematics majors are males. (*c*) Some students are 25 (years) or older.

Use Theorem 4.5 to negate the quantifiers.

(*a*) At least one student does not live in the dormitories. (Some students do not live in the dormitories.)

(*b*) At least one mathematics major is female. (Some mathematics majors are female.)

(*c*) None of the students is 25 or older. (All the students are under 25.)

© The McGraw–Hill Companies, 2004

Supplementary Problems

PROPOSITION AND LOGICAL OPERATIONS

4.22. Let p be "Audrey speaks French" and let q be "Audrey speaks Danish". Give a simple verbal sentence which describes each of the following:

$$(a)\ p \vee q; \quad (b)\ p \wedge q; \quad (c)\ p \wedge \neg q; \quad (d)\ \neg p \vee \neg q; \quad (e)\ \neg \neg p; \quad (f)\ \neg(\neg p \wedge \neg q).$$

4.23. Let p denote "He is rich" and let q denote "He is happy". Write each statement in symbolic form using p and q. Note that "He is poor" and "He is unhappy" are equivalent to $\neg p$ and $\neg q$, respectively.

(*a*) If he is rich, then he is unhappy.

(*b*) He is neither rich nor happy.

(*c*) It is necessary to be poor in order to be happy.

(*d*) To be poor is to be unhappy.

4.24. Find the truth tables for: (*a*) $p \vee \neg q$; (*b*) $\neg p \wedge \neg q$.

4.25. Verify that the proposition $(p \wedge q) \wedge \neg (p \vee q)$ is a contradiction.

ARGUMENTS

4.26. Test the validity of each argument:

(*a*) If it rains, Erik will be sick.
It did not rain.

Erik was not sick.

(*b*) If it rains, Erik will be sick.
Erik was not sick.

It did not rain.

4.27. Test the validity of the following argument:

If I study, then I will not fail mathematics.
If I do not play basketball, then I will study.
But I failed mathematics.

Therefore I must have played basketball.

4.28. Show that: (*a*) $p \wedge q$ logically implies $p \leftrightarrow q$, (*b*) $p \leftrightarrow \neg q$ does not logically imply $p \rightarrow q$.

QUANTIFIERS

4.29. Let $A = \{1, 2, \ldots, 9, 10\}$. Consider each of the following sentences. If it is a statement, then determine its truth value. If it is a propositional function, determine its truth set.

(*a*) $(\forall x \in A)(\exists y \in A)(x + y < 14)$.

(*b*) $(\forall y \in A)(x + y < 14)$.

(*c*) $(\forall x \in A)(\forall y \in A)(x + y < 14)$.

(*d*) $(\exists y \in A)(x + y < 14)$.

4.30. Negate each of the following statements:

(*a*) If the teacher is absent, then some students do not complete their homework.

(*b*) All the students completed their homework and the teacher is present.

(*c*) Some of the students did not complete their homework or the teacher is absent.

4.31. Negate each of the statements in Problem 4.17.

4.32. Find a counterexample for each statement where $\mathbf{U} = \{3, 5, 7, 9\}$ is the universal set: (*a*) $\forall x, x + 3 \geq 7$; (*b*) $\forall x$, x is odd; (*c*) $\forall x$, x is prime; (*d*) $\forall x, |x| = x$.

Answers to Supplementary Problems

4.22. In each case, translate $\wedge$, $\vee$, and $\neg$ to read "and", "or", and "It is false that" or "not", respectively, and then simplify the English sentence.

(*a*) Audrey speaks French or Danish.

(*b*) Audrey speaks French and Danish.

(*c*) Audrey speaks French but not Danish.

(*d*) Audrey does not speak French or she does not speak Danish.

(*e*) It is not true that Audrey does not speak English.

(*f*) It is not true that Audrey speaks neither French nor Danish.

4.23. (*a*) $p \rightarrow \neg q$; (*b*) $\neg p \wedge \neg q$; (*c*) $q \rightarrow \neg p$; (*d*) $\neg p \leftrightarrow \neg q$.

4.24. The truth tables appear in Fig. 4-20.

p	q	$\neg q$	$p \vee \neg q$
T	T	F	T
T	F	T	T
F	T	F	F
F	F	T	T

(*a*)

p	q	$\neg p$	$\neg q$	$\neg p \wedge \neg q$
T	T	F	F	F
T	F	F	T	F
F	T	T	F	F
F	F	T	T	T

(*b*)

Fig. 4-20

4.25. It is a contradiction since its truth table in Fig. 4-21 is false for all values of p and q.

p	q	$p \wedge q$	$p \vee q$	$\neg (p \vee q)$	$(p \wedge q) \wedge \neg (p \vee q)$
T	T	T	T	F	F
T	F	F	T	F	F
F	T	F	T	F	F
F	F	F	F	T	F

Fig. 4-21

4.26. First translate the arguments into symbolic form using, say, p for "It rains" and q for "Erik is sick" as follows:

$$(a)\ p \to q, \neg p \vdash \neg q, \qquad (b)\ p \to q, \neg q \vdash \neg p$$

By Problem 4.12, argument (a) is a fallacy. By Problem 4.13, argument (b) is valid.

4.27. Letting p be "I study", q be "I fail mathematics", and r be "I play basketball", the given argument has the form:

$$p \to \neg q, \neg r \to p, q \vdash r$$

Construct the truth tables as in Fig. 4-22 where the premises $p \to \neg q$, $\neg r \to p$, and q are true simultaneously only in the fifth line of the table, and in that case the conclusion r is also true. Hence the arguments is valid.

p	q	r	$\neg q$	$p \to \neg q$	$\neg r$	$\neg r \to p$
T	T	T	F	F	F	T
T	T	F	F	F	T	T
T	F	T	T	T	F	T
T	F	F	T	T	T	T
F	T	T	F	T	F	T
F	T	F	F	T	T	F
F	F	T	T	T	F	T
F	F	F	T	T	T	F

Fig. 4-22

4.28. (a) Construct the truth tables of $p \wedge q$ and $p \leftrightarrow q$ as in Fig. 4-23(a). Note that $p \wedge q$ is true only in the first line of the table where $p \leftrightarrow q$ is also true.

(b) Construct the truth tables of $p \leftrightarrow \neg q$ and $p \to q$ as in Fig. 4-23(b). Note that $p \leftrightarrow \neg q$ is true in the second line of the table where $p \to q$ is false.

p	q	$p \wedge q$	$p \leftrightarrow q$
T	T	T	T
T	F	F	F
F	T	F	F
F	F	F	T

(a)

p	q	$\neg q$	$p \leftrightarrow \neg q$	$p \to q$
T	T	F	F	T
T	F	T	T	F
F	T	F	T	T
F	F	T	F	T

(b)

Fig. 4-23

4.29. (a) The open sentence in two variables is preceded by two quantifiers; hence it is a statement. Moreover, the statement is true.

(b) The open sentence is preceded by one quantifier; hence it is a propositional function of the other variable. Note that for every $y \in A$, $x_0 + y < 14$ if and only if $x_0 = 1, 2$, or 3. Hence the truth set is $\{1, 2, 3\}$.

(c) It is a statement and it is false: if $x_0 = 8$ and $y_0 = 9$, then $x_0 + y_0 < 14$ is not true.

(d) It is an open sentence in x. The truth set is A itself.

4.30. (a) The teacher is absent and all the students completed their homework.

(b) Some of the students did not complete their homework or the teacher is absent.

(c) All the students completed their homework and the teacher is present.

4.31. (a) $(\forall x \in A)(x + 3 \neq 10)$.

(b) $(\exists x \in A)(x + 3 \geq 10)$.

(c) $(\forall x \in A)(x + 3 \geq 5)$.

(d) $(\exists x \in A)(x + 3 > 7)$.

4.32. (*a*) Here 5, 7, and 9 are counterexamples.
(*b*) The statement is true; hence no counterexample exists.
(*c*) Here 9 is the only counterexample.
(*d*) The statement is true; hence there is no counterexample.

© The McGraw–Hill Companies, 2004

Chapter 5

Vectors and Matrices

5.1 INTRODUCTION

Data is frequently arranged in *arrays*, that is, sets whose elements are indexed by one or more subscripts. Frequently, a one-dimensional array is called a vector and a two-dimensional array is called a matrix. (The dimension, in this case, denotes the number of subscripts.) Here we motivate these objects and their notation.

Suppose the weights (in pounds) of eight students are listed as follows:

$$134, \quad 156, \quad 127, \quad 145, \quad 203, \quad 186, \quad 145, \quad 138$$

One can denote all the values in the list using only one symbol, say w, but with different subscripts:

$$w_1, \quad w_2, \quad w_3, \quad w_4, \quad w_5, \quad w_6, \quad w_7, \quad w_8$$

Observe that each subscript denotes the position of the value in the list. For example,

$$w_1 = 134, \text{ the first number;} \qquad w_2 = 156, \text{ the second number;} \qquad \ldots$$

Such a list of values is called a *vector* or *linear array*.

Using this subscript notation, one can write the sum S and the average A of the weights as follows:

$$S = \sum_{k=1}^{8} w_k = w_1 + w_2 + \ldots + w_8 \qquad \text{and} \qquad A = \frac{S}{8} = \frac{1}{8}\left[\sum_{k=1}^{8} w_k\right]$$

Subscript notation is indispensable in developing concise expressions for arithmetic manipulations of lists of values.

Similarly, a chain of 28 stores, each store having four departments, could list its weekly sales (say, to the nearest dollar) as in Table 5-1. We need only one symbol, say s, with two subscripts to denote all the values in the table:

$$s_{1,1}, \quad s_{1,2}, \quad s_{1,3}, \quad s_{1,4}, \quad s_{2,1}, \quad s_{2,2}, \quad \ldots, \quad s_{28,4}$$

where $s_{i,j}$ denotes the sales in store i, department j. (We write s_{ij} instead of $s_{i,j}$ when there is no possibility of misunderstanding.) Thus,

$$s_{11} = \$2872, \quad s_{12} = \$805, \quad s_{13} = \$3211, \quad \ldots$$

Such a rectangular array of numbers is called a *matrix* or a *two-dimensional array*.

This chapter investigates vectors and matrices and certain algebraic operations involving them. In such a context, the numbers themselves are called *scalars*.

Table 5-1

Store \ Dept.	1	2	3	4
1	2872	805	3211	1560
2	2196	1223	2525	1744
3	3257	1017	3686	1951
. . .	. . .	. . .	. . .	. . .
28	2618	931	2333	982

5.2 VECTORS

By a *vector* u, we mean a list of numbers, say, $a_1, a_2, \ldots, a_n$. Such a vector is denoted by

$$u = (a_1, a_2, \ldots, a_n)$$

The numbers a_i are called the *components* or *entries* of u. If all the $a_i = 0$, then u is called the *zero vector*. Two such vectors, u and v, are *equal*, written $u = v$, if they have the same number of components *and* corresponding components are equal.

EXAMPLE 5.1

(*a*) The following are vectors:

$$(3, -4) \qquad (6, 8) \qquad (0, 0, 0) \qquad (2, 3, 4)$$

The first two vectors have two components, whereas the last two vectors have three components. The third vector is the zero vector with three components.

(*b*) Although the vectors $(1, 2, 3)$ and $(2, 3, 1)$ contain the same numbers, they are not equal, since corresponding components are not equal.

Vector Operations

Consider two arbitrary vectors u and v with the same number of components, say

$$u = (a_1, a_2, \ldots, a_n) \qquad \text{and} \qquad v = (b_1, b_2, \ldots, b_n)$$

The *sum* of u and v, written $u + v$, is the vector obtained by adding corresponding components from u and v; that is,

$$u + v = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n)$$

The *scalar product* or, simply, *product*, of a scalar k and the vector u, written ku, is the vector obtained by multiplying each component of u by k; that is,

$$ku = (ka_1, ka_2, \ldots, ka_n)$$

We also define

$$-u = -1(u) \qquad \text{and} \qquad u - v = u + (-v)$$

and we let 0 denote the zero vector. The vector $-u$ is called the *negative* of the vector u.

The *dot product* or *inner product* of the above vectors u and v is denoted and defined by

$$u \cdot v = a_1 b_1 + a_2 b_2 + \cdots + a_n b_n$$

The *norm* or *length* of the vector u is denoted and defined by

$$\|u\| = \sqrt{u \cdot u} = \sqrt{a_1^2 + a_2^2 + \cdots + a_n^2}$$

We note that $\|u\| = 0$ if and only if $u = 0$; otherwise $\|u\| > 0$.

EXAMPLE 5.2 Let $u = (2, 3, -4)$ and $v = (1, -5, 8)$. Then

$$\begin{aligned} u + v &= (2 + 1, 3 - 5, -4 + 8) = (3, -2, 4) \\ 5u &= (5 \cdot 2,\ 5 \cdot 3,\ 5 \cdot (-4)) = (10, 15, -20) \\ -v &= -1 \cdot (1, -5, 8) = (-1, 5, -8) \\ 2u - 3v &= (4, 6, -8) + (-3, 15, -24) = (1, 21, -32) \\ u \cdot v &= 2 \cdot 1 + 3 \cdot (-5) + (-4) \cdot 8 = 2 - 15 - 32 = -45 \\ \|u\| &= \sqrt{2^2 + 3^2 + (-4)^2} = \sqrt{4 + 9 + 16} = \sqrt{29} \end{aligned}$$

Vectors under the operations of vector addition and scalar multiplication have various properties, e.g.,

$$k(u+v) = ku + kv$$

where k is a scalar and u and v are vectors. Many such properties appear in Theorem 5.1 (see Section 5.4), which also holds for vectors since vectors may be viewed as a special case of matrices.

Column Vectors

Sometimes a list of numbers is written vertically rather than horizontally, and the list is called a *column vector*. In this context, the above horizontally written vectors are called *row vectors*. The above operations for row vectors are defined analogously for column vectors.

EXAMPLE 5.3

(*a*) The following are column vectors:

$$\begin{bmatrix} 0 \\ 1 \end{bmatrix}, \quad \begin{bmatrix} 1 \\ -3 \end{bmatrix}, \quad \begin{bmatrix} 1 \\ 2 \\ -6 \end{bmatrix}, \quad \begin{bmatrix} 1.4 \\ \frac{3}{4} \\ -19 \end{bmatrix}$$

The first two vectors have two components, whereas the last two have three components.

(*b*) Let

$$u = \begin{bmatrix} 5 \\ 3 \\ -4 \end{bmatrix} \quad \text{and} \quad v = \begin{bmatrix} 3 \\ -1 \\ -2 \end{bmatrix}$$

Then

$$2u - 3v = \begin{bmatrix} 10 \\ 6 \\ -8 \end{bmatrix} + \begin{bmatrix} -9 \\ 3 \\ 6 \end{bmatrix} = \begin{bmatrix} 1 \\ 9 \\ -2 \end{bmatrix}$$

$$u \cdot v = 15 - 3 + 8 = 20 \quad \text{and} \quad \|u\| = \sqrt{25 + 9 + 16} = \sqrt{50} = 5\sqrt{2}$$

.

5.3 MATRICES

A *matrix* A is a rectangular array of numbers usually presented in the form

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}$$

The m horizontal lists of numbers are called the *rows* of A, and the n vertical lists of numbers its *columns*. Thus the element a_{ij}, called the *ij entry*, appears in row i and column j. We frequently denote such a matrix by simply writing $A = [a_{ij}]$.

A matrix with m rows and n columns is called an m *by* n matrix, written $m \times n$. The pair of numbers m and n is called the *size* of the matrix. Two matrices A and B are equal, written $A = B$, if they have the same size and if corresponding elements are equal. Thus, the equality of two $m \times n$ matrices is equivalent to a system of mn equalities, one for each corresponding pair of elements.

A matrix with only one row is called a *row matrix* or *row vector*, and a matrix with only one column is called a *column matrix* or *column vector*. A matrix whose entries are all zero is called a *zero matrix* and will usually be denoted by 0.

EXAMPLE 5.4

(*a*) The rectangular array $A = \begin{bmatrix} 1 & -4 & 5 \\ 0 & 3 & -2 \end{bmatrix}$ is a 2×3 matrix. Its rows are $[1, -4, 5]$ and $[0, 3, -2]$, and its columns are $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$, $\begin{bmatrix} -4 \\ 3 \end{bmatrix}$, $\begin{bmatrix} 5 \\ -2 \end{bmatrix}$.

(*b*) The 2×4 zero matrix is the matrix $0 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$.

(*c*) Suppose

$$\begin{bmatrix} x+y & 2z+t \\ x-y & z-t \end{bmatrix} = \begin{bmatrix} 3 & 7 \\ 1 & 5 \end{bmatrix}$$

Then the four corresponding entries must be equal. That is,

$$x + y = 3, \qquad x - y = 1, \qquad 2z + t = 7, \qquad z - t = 5$$

The solution of the system of equations is

$$x = 2, \qquad y = 1, \qquad z = 4, \qquad t = -1$$

5.4 MATRIX ADDITION AND SCALAR MULTIPLICATION

Let $A = [a_{ij}]$ and $B = [b_{ij}]$ be two matrices of the same size, say, $m \times n$ matrices. The *sum* of A and B, written $A + B$, is the matrix obtained by adding corresponding elements from A and B. That is,

$$A + B = \begin{bmatrix} a_{11} + b_{11} & a_{12} + b_{12} & \cdots & a_{1n} + b_{1n} \\ a_{21} + b_{21} & a_{22} + b_{22} & \cdots & a_{2n} + b_{2n} \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ a_{m1} + b_{m1} & a_{m2} + b_{m2} & \cdots & a_{mn} + b_{mn} \end{bmatrix}$$

The *product* of the matrix A by a scalar k, written $k \cdot A$ or simply kA, is the matrix obtained by multiplying each element of A by k. That is,

$$kA = \begin{bmatrix} ka_{11} & ka_{12} & \cdots & ka_{1n} \\ ka_{21} & ka_{22} & \cdots & ka_{2n} \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ ka_{m1} & ka_{m2} & \cdots & ka_{mn} \end{bmatrix}$$

Observe that $A + B$ and kA are also $m \times n$ matrices. We also define

$$-A = (-1)A \qquad \text{and} \qquad A - B = A + (-B)$$

The matrix $-A$ is called the *negative* of the matrix A. The sum of matrices with different sizes is not defined.

EXAMPLE 5.5 Let $A = \begin{bmatrix} 1 & -2 & 3 \\ 0 & 4 & 5 \end{bmatrix}$ and $B = \begin{bmatrix} 4 & 6 & 8 \\ 1 & -3 & -7 \end{bmatrix}$. Then

$$A + B = \begin{bmatrix} 1+4 & -2+6 & 3+8 \\ 0+1 & 4+(-3) & 5+(-7) \end{bmatrix} = \begin{bmatrix} 5 & 4 & 11 \\ 1 & 1 & -2 \end{bmatrix}$$

$$3A = \begin{bmatrix} 3(1) & 3(-2) & 3(3) \\ 3(0) & 3(4) & 3(5) \end{bmatrix} = \begin{bmatrix} 3 & -6 & 9 \\ 0 & 12 & 15 \end{bmatrix}$$

$$2A - 3B = \begin{bmatrix} 2 & -4 & 6 \\ 0 & 8 & 10 \end{bmatrix} + \begin{bmatrix} -12 & -18 & -24 \\ -3 & 9 & 21 \end{bmatrix} = \begin{bmatrix} -10 & -22 & -18 \\ -3 & 17 & 31 \end{bmatrix}$$

Matrices under matrix addition and scalar multiplication have the following properties.

Theorem 5.1: Let A, B, C be matrices with the same size, and let k and k' be scalars. Then:

(i) $(A + B) + C = A + (B + C)$ (v) $k(A + B) = kA + kB$.
(ii) $A + 0 = 0 + A$ (vi) $(k + k')A = kA + k'A$.
(iii) $A + (-A) = (-A) + 0 = A$ (vii) $(kk')A = k(k'A)$.
(iv) $A + B = B + A$ (viii) $1A = A$.

Note first that the 0 in (ii) and (iii) refers to the zero matrix. Also, by (i) and (iv), any sum of matrices

$$A_1 + A_2 + \cdots + A_n$$

requires no parentheses, and the sum does not depend on the order of the matrices. Furthermore, using (vi) and (viii), we also have

$$A + A = 2A, \qquad A + A + A = 3A, \qquad \ldots$$

Lastly, since n-component vectors may be identified with either $1 \times n$ or $n \times 1$ matrices, Theorem 5.1 also holds for vectors under vector addition and scalar multiplication.

The proof of Theorem 5.1 reduces to showing that the ij entries on both sides of each matrix equation are equal. (See Problem 5.10.)

5.5 MATRIX MULTIPLICATION

The product of matrices A and B, written AB, is somewhat complicated. For this reason, we first begin with a special case. (The reader is referred to Section 3.5 for a discussion of the summation symbol Σ, the Greek capital letter sigma.)

The product AB of a row matrix $A = [a_i]$ and a column matrix $B = [b_i]$ with the same number of elements is defined as follows:

$$AB = [a_1, a_2, \ldots, a_n]\begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix} = a_1b_1 + a_2b_2 + \cdots + a_nb_n = \sum_{k=1}^{n} a_kb_k$$

That is, AB is obtained by multiplying corresponding entries in A and B and then adding all the products. We emphasize that AB is a scalar (or a 1×1 matrix). The product AB is not defined when A and B have different numbers of elements.

EXAMPLE 5.6

(*a*) $[7, -4, 5]\begin{bmatrix} 3 \\ 2 \\ -1 \end{bmatrix} = 7(3) + (-4)(2) + 5(3) = 21 - 8 - 5 = 8$

(*b*) $[6, -1, 8, 3]\begin{bmatrix} 4 \\ -9 \\ -2 \\ 5 \end{bmatrix} = 24 + 9 - 16 + 15 = 32$

We are now ready to define matrix multiplication in general.

Definition: Suppose $A = [a_{ik}]$ and $B = [b_{kj}]$ are matrices such that the number of columns of A is equal to the number of rows of B; say, A is a $m \times p$ matrix and B is a $p \times n$ matrix. Then the product AB is the $m \times n$ matrix whose ij-entry is obtained by multiplying the ith row of A by the jth column of B. That is,

$$\begin{bmatrix} a_{11} & \cdots & a_{1p} \\ \cdot & \cdots & \cdot \\ a_{i1} & \cdots & a_{ip} \\ \cdot & \cdots & \cdot \\ a_{m1} & \cdots & a_{mp} \end{bmatrix} \begin{bmatrix} b_{11} & \cdots & b_{1j} & \cdots & b_{1n} \\ \cdot & \cdots & \cdot & \cdots & \cdot \\ \cdot & \cdots & \cdot & \cdots & \cdot \\ \cdot & \cdots & \cdot & \cdots & \cdot \\ b_{p1} & \cdots & b_{pj} & \cdots & b_{pn} \end{bmatrix} = \begin{bmatrix} c_{11} & \cdots & c_{1n} \\ \cdot & \cdots & \cdot \\ \cdot & c_{ij} & \cdot \\ \cdot & \cdots & \cdot \\ c_{m1} & \cdots & c_{mn} \end{bmatrix}$$

where

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{ip}b_{pj} = \sum_{k=1}^{p} a_{ik}b_{kj}$$

We emphasize that the product AB is not defined if A is an $m \times p$ matrix and B is a $q \times n$ matrix, where $p \neq q$.

EXAMPLE 5.7

(*a*) Find AB where $A = \begin{bmatrix} 1 & 3 \\ 2 & -1 \end{bmatrix}$ and $B = \begin{bmatrix} 2 & 0 & -4 \\ 5 & -2 & 6 \end{bmatrix}$.

Since A is 2×2 and B is 2×3, the product AB is defined and AB is a 2×3 matrix. To obtain the first row of the product matrix AB, multiply the first row $(1, 3)$ of A times each column of B,

$$\begin{bmatrix} 2 \\ 5 \end{bmatrix}, \quad \begin{bmatrix} 0 \\ -2 \end{bmatrix}, \quad \begin{bmatrix} -4 \\ 6 \end{bmatrix}$$

respectively. That is,

$$AB = \begin{bmatrix} 2+15 & 0-6 & -4+18 \\ & & \end{bmatrix} = \begin{bmatrix} 17 & -6 & 14 \\ & & \end{bmatrix}$$

To obtain the second row of the product AB, multiply the second row $(2, -1)$ of A times each column of B, respectively. Thus

$$AB = \begin{bmatrix} 17 & -6 & 14 \\ 4-5 & 0+2 & -8-6 \end{bmatrix} = \begin{bmatrix} 17 & -6 & 14 \\ -1 & 2 & -14 \end{bmatrix}$$

(*b*) Suppose $A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$ and $B = \begin{bmatrix} 5 & 6 \\ 0 & -2 \end{bmatrix}$. Then

$$AB = \begin{bmatrix} 5+0 & 6-4 \\ 15+0 & 18-8 \end{bmatrix} = \begin{bmatrix} 5 & 2 \\ 15 & 10 \end{bmatrix} \quad \text{and} \quad BA = \begin{bmatrix} 5+18 & 10+24 \\ 0-6 & 0-8 \end{bmatrix} = \begin{bmatrix} 23 & 34 \\ -6 & -8 \end{bmatrix}$$

The above Example 5.6(*b*) shows that matrix multiplication is not commutative, i.e., the products AB and BA of matrices need not be equal.

Matrix multiplication does, however, satisfy the following properties:

Theorem 5.2: Let A, B, C be matrices. Then, whenever the products and sums are defined:

(i) $(AB)C = A(BC)$ (associative law).
(ii) $A(B + C) = AB + AC$ (left distributive law).
(iii) $(B + C)A = BA + CA$ (right distributive law).
(iv) $k(AB) = (kA)B = A(kB)$ where k is a scalar.

We note that $0A = 0$ and $B0 = 0$ where 0 is the zero matrix.

Matrix Multiplication and Systems of Linear Equations

Any system S of linear equations is equivalent to the matrix equation

$$AX = B$$

where A is the matrix consisting of the coefficients, X is the column vector of unknowns, and B is the column vector of constants. (Here *equivalent* means that any solution of the system S is a solution to the matrix equation $AX = B$, and vice versa.) For example, the system

$$\begin{aligned} x + 2y - 3z &= 4 \\ 5x - 6y + 8z &= 9 \end{aligned} \quad \text{is equivalent to} \quad \begin{bmatrix} 1 & 2 & -3 \\ 5 & -6 & 8 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 4 \\ 9 \end{bmatrix}$$

Observe that the system is completely determined by the matrix

$$M = [A, B] = \begin{bmatrix} 1 & 2 & -3 & 4 \\ 5 & -6 & 8 & 9 \end{bmatrix}$$

which is called the *augmented matrix* of the system.

5.6 TRANSPOSE

The *transpose* of a matrix A, written A^T, is the matrix obtained by writing the rows of A, in order, as columns. For example,

$$\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix}^T = \begin{bmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{bmatrix} \quad \text{and} \quad [1, -3, -5]^T = \begin{bmatrix} 1 \\ -3 \\ -5 \end{bmatrix}$$

Note that if A is an $m \times n$ matrix, then A^T is an $n \times m$ matrix. In particular, the transpose of a row vector is a column vector, and vice versa. Furthermore, if $B = [b_{ij}]$ is the transpose of $A = [a_{ij}]$, then $b_{ij} = a_{ji}$ for all i and j.

The transpose operation on matrices satisfies the following properties.

Theorem 5.3: Let A and B be matrices and k be a scalar. Then, whenever the sum and products are defined:

(i) $(A + B)^T = A^T + B^T$.
(ii) $(kA)^T = kA^T$, for k a scalar.
(iii) $(AB)^T = B^T A^T$.
(iv) $(A^T)^T = A$.

We emphasize that, by (iii), the transpose of a product is the product of the transposes, but in the reverse order.

5.7 SQUARE MATRICES

A matrix with the same number of rows as columns is called a *square matrix*. A square matrix with n rows and n columns is said to be of *order n*, and is called an *n-square matrix*.

The *main diagonal*, or simply *diagonal*, of an n-square matrix $A = [a_{ij}]$ consists of the elements $a_{11}, a_{22}, \ldots, a_{nn}$.

The n-square *unit matrix*, denoted by I_n or simply I, is the square matrix with ones along the diagonal and zeros elsewhere. The unit matrix I plays the same role in matrix multiplication as the number 1 does in the usual multiplication of numbers. Specifically,

$$AI = IA = A$$

for any square matrix.

Consider, for example, the matrices

$$\begin{bmatrix} 1 & -2 & 0 \\ 0 & -4 & -6 \\ 5 & 3 & 2 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Both are square matrices. The first matrix is of order 3 and its diagonal consists of the elements 1, -4, and 2. The second matrix is of order 4; its diagonal consists only of ones, and there are only zeros elsewhere. Thus the second matrix is the unit matrix of order 4.

Algebra of Square Matrices

Let A be any square matrix. Then we can multiply A by itself. In fact, we can form all nonnegative *powers* of A as follows:

$$A^2 = AA, \qquad A^3 = A^2A, \qquad \ldots, \qquad A^{n+1} = A^nA, \qquad \ldots, \qquad \text{and} \qquad A^0 = I \text{ (when } A \neq 0)$$

Polynomials in the matrix A are also defined. Specifically, for any polynomial

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$$

where the a_i are scalars, we define $f(A)$ to be the matrix

$$f(A) = a_0I + a_1A + a_2A^2 + \cdots + a_nA^n$$

Note that $f(A)$ is obtained from $f(x)$ by substituting the matrix A for the variable x and substituting the scalar matrix a_0I for the scalar term a_0. In the case that $f(A)$ is the zero matrix, the matrix A is then called a *zero* or *root* of the polynomial $f(x)$.

EXAMPLE 5.8 Suppose $A = \begin{bmatrix} 1 & 2 \\ 3 & -4 \end{bmatrix}$. Then

$$A^2 = \begin{bmatrix} 1 & 2 \\ 3 & -4 \end{bmatrix}\begin{bmatrix} 1 & 2 \\ 3 & -4 \end{bmatrix} = \begin{bmatrix} 7 & -6 \\ -9 & 22 \end{bmatrix} \quad \text{and} \quad A^3 = A^2A = \begin{bmatrix} 7 & -6 \\ -9 & 22 \end{bmatrix}\begin{bmatrix} 1 & 2 \\ 3 & -4 \end{bmatrix} = \begin{bmatrix} -11 & 38 \\ 57 & -106 \end{bmatrix}$$

Suppose $f(x) = 2x^2 - 3x + 5$. Then

$$f(A) = 2\begin{bmatrix} 7 & -6 \\ -9 & 22 \end{bmatrix} - 3\begin{bmatrix} 1 & 2 \\ 3 & -4 \end{bmatrix} + 5\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 16 & -18 \\ -27 & 61 \end{bmatrix}$$

Suppose $g(x) = x^2 + 3x - 10$. Then

$$g(A) = \begin{bmatrix} 7 & -6 \\ -9 & 22 \end{bmatrix} + 3\begin{bmatrix} 1 & 2 \\ 3 & -4 \end{bmatrix} - 10\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

Thus A is a zero of the polynomial $g(x)$.

5.8 INVERTIBLE (NONSINGULAR) MATRICES, INVERSES

A square matrix A is said to be *invertible* (or *nonsingular*) if there exists a matrix B with the property that:

$$AB = BA = I, \qquad \text{the identity matrix}$$

Such a matrix B is unique (Problem 5.24); it is called the *inverse* of A and is denoted by A^{-1}. Observe that B is the inverse of A if and only if A is the inverse of B. For example, suppose

$$A = \begin{bmatrix} 2 & 5 \\ 1 & 3 \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} 3 & -5 \\ -1 & 2 \end{bmatrix}$$

Then

$$AB = \begin{bmatrix} 6-5 & -10+10 \\ 3-3 & -5+6 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \text{and} \quad BA = \begin{bmatrix} 6-5 & 15-15 \\ -2+2 & -5+6 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Thus A and B are inverses.

It is known that $AB = I$ if and only if $BA = I$; hence it is necessary to test only one product to determine whether two given matrices are inverses, as in the next example.

EXAMPLE 5.9

$$\begin{bmatrix} 1 & 0 & 2 \\ 2 & -1 & 3 \\ 4 & 1 & 8 \end{bmatrix} \begin{bmatrix} -11 & 2 & 2 \\ -4 & 0 & 1 \\ 6 & -1 & -1 \end{bmatrix} = \begin{bmatrix} -11+0+12 & 2+0-2 & 2+0-2 \\ -22+4+18 & 4+0-3 & 4-1-3 \\ -44-4+48 & 8+0-8 & 8+1-8 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Thus the two matrices are invertible and are inverses of each other.

5.9 DETERMINANTS

To each n-square matrix $A = [a_{ij}]$ we assign a specific number called the *determinant* of A and denoted by $\det(A)$ or $|A|$ or

$$\begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix}$$

We emphasize that a square array of numbers enclosed by straight lines, called a *determinant of order n*, is not a matrix but denotes the number that the determinant function assigns to the enclosed array of numbers, i.e., the enclosed square matrix.

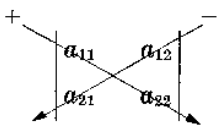
The determinants of order 1, 2, and 3 are defined as follows:

$$|a_{11}| = a_{11}$$

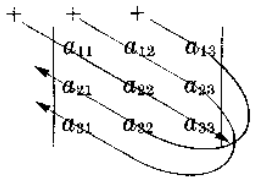
$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}a_{22} - a_{12}a_{21}$$

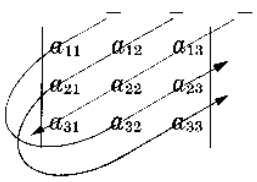
$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31} - a_{12}a_{21}a_{33} - a_{11}a_{23}a_{32}$$

The following diagram may help the reader remember the determinant of order 2:



That is, the determinant equals the product of the elements along the plus-labeled arrow minus the product of the elements along the minus-labeled arrow. There is an analogous way to remember a determinant of order 3. For notational convenience we have separated the plus-labeled and minus-labeled arrows:





We emphasize that there are no such diagrammatic tricks to remember determinants of higher order.

EXAMPLE 5.10

(*a*) $\begin{vmatrix} 5 & 4 \\ 2 & 3 \end{vmatrix} = 5(3) - 4(2) = 15 - 8 = 7, \qquad \begin{vmatrix} 2 & 1 \\ -4 & 6 \end{vmatrix} = 2(6) - 1(-4) = 12 + 4 = 16.$

(*b*) $$\begin{vmatrix} 2 & 1 & 3 \\ 4 & 6 & -1 \\ 5 & 1 & 0 \end{vmatrix} = 2(6)(0) + 1(-1)(5) + 3(1)(4) - 3(6)(5) - 1(4)(0) - 2(1)(-1)$$
$$= 0 - 5 + 12 - 90 - 0 + 2 = -81.$$

General Definition of Determinants

The general definition of a determinant of order n is as follows:

$$\det(A) = \sum \operatorname{sgn}(\sigma) a_{1j_1} a_{2j_2} \cdots a_{nj_n}$$

where the sum is taken over all permutations $\sigma = \{j_1, j_2, \ldots, j_n\}$ of $\{1, 2, \ldots, n\}$. Here sgn (σ) equals $+1$ or -1 according as an even or an odd number of interchanges are required to change σ so that its numbers are in the usual order. We have included the general definition of the determinant function for completeness. The reader is referred to texts in matrix theory or linear algebra for techniques for computing determinants of order greater than 3. Permutations are studied in Chapter 6.

An important property of the determinant function is that it is multiplicative. That is:

Theorem 5.4: Let A and B be any n-square matrices. Then

$$\det(AB) = \det(A) \cdot \det(B)$$

The proof of the above theorem lies beyond the scope of this text.

Determinants and Inverses of 2 × 2 Matrices

Let A be an arbitrary 2×2 matrix, say,

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

We want to derive a formula for A^{-1}, the inverse of A. Specifically, we seek $2^2 = 4$ scalars, say x_1, y_1, x_2, y_2, such that

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x_1 & x_2 \\ y_1 & y_2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \text{or} \quad \begin{bmatrix} ax_1 + by_1 & ax_2 + by_2 \\ cx_1 + dy_1 & cx_2 + dy_2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Setting the four entries equal, respectively, to the corresponding entries in the identity matrix yields four equations which can be partitioned into two 2×2 systems as follows:

$$ax_1 + by_1 = 1, \qquad ax_2 + by_2 = 0,$$
$$cx_1 + dy_1 = 0, \qquad cx_2 + dy_2 = 1$$

Observe that the augmented matrices of the two systems are as follows:

$$\begin{bmatrix} a & b & 1 \\ c & d & 0 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} a & b & 0 \\ c & d & 1 \end{bmatrix}$$

(Note that the original matrix A is the coefficient matrix of both systems.)

Suppose now $|A| = ad - bc \neq 0$. Then we can uniquely solve the two systems for the unknowns x_1, y_1, x_2, y_2 obtaining

$$x_1 = \frac{d}{ad-bc} = \frac{d}{|A|}, \qquad y_1 = \frac{-c}{ad-bc} = \frac{-c}{|A|}, \qquad x_2 = \frac{-b}{ad-bc} = \frac{-b}{|A|}, \qquad y_2 = \frac{a}{ad-bc} = \frac{a}{|A|}$$

Accordingly,

$$A^{-1} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \begin{bmatrix} d/|A| & -b/|A| \\ -c/|A| & a/|A| \end{bmatrix} = \frac{1}{|A|}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

In words: When $|A| \neq 0$, the inverse of a 2×2 matrix A is obtained as follows:

(1) Interchange the elements on the main diagonal.
(2) Take the negatives of the other elements.
(3) Multiply the matrix by $1/|A|$ or, equivalently, divide each element by $|A|$.

For example, if $A = \begin{bmatrix} 2 & 3 \\ 4 & 5 \end{bmatrix}$, then $|A| = -2$ and so

$$A^{-1} = \frac{1}{-2}\begin{bmatrix} 5 & -3 \\ -4 & 2 \end{bmatrix} = \begin{bmatrix} -\frac{5}{2} & \frac{8}{2} \\ 2 & -1 \end{bmatrix}$$

On the other hand, if $|A| = 0$, then we cannot solve for the unknowns x_1, y_1, x_2, y_2, and A^{-1} would not exist. Although there is no simple formula for inverses of matrices of higher order, this result does hold true in general. Namely,

Theorem 5.5: A matrix A is invertible if and only if it has a nonzero determinant.

5.10 ELEMENTARY ROW OPERATIONS, GAUSSIAN ELIMINATION (OPTIONAL)

This section discusses the Gaussian elimination algorithm in the context of elementary row operations.

Elementary Row Operations

Consider a matrix $A = [a_{ij}]$ whose rows will be denoted, respectively, by R_1, R_2, ..., R_m. The first nonzero element in a row R_i is called the *leading* nonzero element. A row with all zeros is called a *zero row*. Thus a zero row has no leading nonzero element.

The following operations on A are called the *elementary row operations*:

[$\mathbf{E}_1$] Interchange row R_i and row R_j. This operation will be indicated by writing: "Interchange R_i and R_j".

[$\mathbf{E}_2$] Multiply each element in a row R_i by a nonzero constant k. This operation will be indicated by writing: "Multiply R_i by k".

[$\mathbf{E}_3$] Add a multiple of one row R_i to another row R_j or, in other words, replace R_j by the sum $kR_i + R_j$. This operation will be indicated by writing: "Add kR_i to R_j".

To avoid fractions, we may perform [$\mathbf{E_2}$] and [$\mathbf{E_3}$] in one step; that is, we may apply the following operation:

[**E**] Add a multiple of one row R_i to a nonzero multiple of another row R_j or, in other words, replace R_j by the sum $kR_i + k'R_j$ where $k' \neq 0$. We indicate this operation by writing: "Add kR_i to $k'R_j$".

We emphasize that, in the row operations [$\mathbf{E_3}$] and [**E**], only row R_j is actually changed.

Notation: Matrices A and B are said to be *row equivalent*, written $A \sim B$, if matrix B can be obtained from matrix A by using elementary row operations.

Echelon Matrices

A matrix A is called an *echelon matrix*, or is said to be in *echelon form*, if the following two conditions hold:

(i) All zero rows, if any, are on the bottom of the matrix.

(ii) Each leading nonzero entry is to the right of the leading nonzero entry in the preceding row.

The matrix is said to be in *row canonical form* if it has the following two additional properties:

(iii) Each leading nonzero entry is 1.

(vi) Each leading nonzero entry is the only nonzero entry in its column.

The zero matrix 0, for any number of rows or columns, is a special example of a matrix in row canonical form. The n-square identity matrix I_n is another example of a matrix in row canonical form.

A square matrix A is said to be in *triangular form* if its diagonal entries $a_{11}, a_{22}, \ldots, a_{nn}$ are the leading nonzero entries. Thus a square matrix in triangular form is a special case of an echelon matrix. The identity matrix I is the only example of a square matrix which is in triangular form and in row canonical form.

EXAMPLE 5.11 The following are echelon matrices whose leading nonzero entries have been circled:

$$\begin{bmatrix} \textcircled{2} & 3 & 2 & 0 & 4 & 5 & -6 \\ 0 & 0 & \textcircled{1} & 1 & -3 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & \textcircled{6} & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} \textcircled{1} & 2 & 3 \\ 0 & 0 & \textcircled{1} \\ 0 & 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & \textcircled{1} & 3 & 0 & 0 & 4 \\ 0 & 0 & 0 & \textcircled{1} & 0 & -3 \\ 0 & 0 & 0 & 0 & \textcircled{1} & 2 \end{bmatrix}, \quad \begin{bmatrix} \textcircled{2} & 4 & 7 \\ 0 & \textcircled{5} & 8 \\ 0 & 0 & \textcircled{6} \end{bmatrix}$$

(The zeros preceding and below the leading nonzero entries in an echelon matrix form a "staircase" pattern as indicated above by the shading.) The third matrix is in row canonical form. The second matrix is not in row canonical form since the third column contains a leading nonzero entry and another nonzero entry. The first matrix is not in row canonical form since some leading nonzero entries are not 1. The last matrix is in triangular form.

Gaussian Elimination in Matrix Form

Consider any matrix A. Two algorithms are given below. The first algorithm transforms the matrix A into an echelon form (using only elementary row operations), and the second algorithm transforms the echelon matrix into a matrix in row canonical form. (The two algorithms together are called *Gaussian elimination*.)

Algorithm 5.10A (**Forward Elimination**): The input is an arbitrary matrix $A = [a_{ij}]$.

Step 1. Find the first column with a nonzero entry. If no such column exists, then EXIT. (We have the zero matrix.) Otherwise, let j_1 denote the number of this column.
(*a*) Arrange so that $a_{1j_1} \neq 0$. That is, if necessary, interchange rows so that a nonzero entry appears in the first row in column j_1.
(*b*) Use a_{1j_1} as a *pivot* to obtain zeros below a_{1j_1}. That is, for $i > 1$:
(1) Set $m = -a_{ij_1}/a_{1j_1}$.
(2) Add aL_1 to L_i.
[This replaces row R_i by $-(a_{ij_1}/a_{1j_1})R_1 + R_i$.]

Step 2. Repeat Step 1 with the submatrix formed by all the rows, excluding the first row. Here we let j_2 denote the first column in the submatrix with a nonzero entry. Hence, at the end of Step 2, we have $a_{2j_2} \neq 0$.

Step 3 to r+1. Continue the above process until the submatrix has no nonzero entry.

We emphasize that at the end of the algorithm the *pivot* (leading nonzero) entries will be

$$a_{1j_1}, a_{2j_2}, \ldots, a_{rj_r}$$

where r denotes the number of nonzero rows in the matrix in echelon form.

Remark 1: The number in Step 1(*b*),

$$m = -\frac{a_{i1}}{a_{11}} = -\frac{\text{coefficient to be deleted}}{\text{pivot}}$$

is called the *multiplier*.

Remark 2: One could replace the operation in Step 1(*b*) by

"Add $-a_{ij_1}R_1$ to $a_{1j_1}R_i$"

This would avoid fractions if all the scalars were originally integers.

Algorithm 5.10B (**Backward Elimination**): The input is a matrix $A = [a_{ij}]$ in echelon form with pivot entries $a_{1j_1}, a_{2j_2}, \ldots a_{rj_r}$

Step 1. (*a*) Multiply the last nonzero row R_r by $1/a_{rj_r}$ so that the pivot entry is equal to 1.
(*b*) Use $a_{rj_r} = 1$ to obtain zeros above the pivot. That is, for $i = r-1, r-2, \ldots, 1$:
(1) Set $m = -a_{ir_i}$.
(2) Add mR_r to R_i.
In other words, apply the elementary row operations

"Add $-a_{ir_1}R_r$ to R_i"

[This replaces row R_i by $-a_{ir_i}R_r + R_i$.]

Step 2 to r − 1. Repeat Step 1 for rows $R_{r-1}, R_{r-2}, \ldots, R_2$.

Step r. Multiply R_1 by $1/a_{1j_1}$.

EXAMPLE 5.12 Find the row canonical form of

$$A = \begin{bmatrix} 1 & 2 & -3 & 1 & 2 \\ 2 & 4 & -4 & 6 & 10 \\ 3 & 6 & -6 & 9 & 13 \end{bmatrix}.$$

First reduce A to echelon form using Algorithm 10.5A. Specifically, use $a_{11} = 1$ as a pivot to obtain zeros below a_{11}, that is, apply the row operations "Add $-2R_1$ to R_2" and "Add $-3R_1$ to R_3. Then use $a_{23} = 2$ as a pivot to obtain 0 below a_{23}, that is, apply the row operation "Add $-\frac{3}{2}R_2$ to R_3." This yields

$$A \sim \begin{bmatrix} 1 & 2 & -3 & 1 & 2 \\ 0 & 0 & 2 & 4 & 6 \\ 0 & 0 & 3 & 6 & 7 \end{bmatrix} \sim \begin{bmatrix} 1 & 2 & -3 & 1 & 2 \\ 0 & 0 & 2 & 4 & 6 \\ 0 & 0 & 0 & 0 & -2 \end{bmatrix}$$

The matrix A is now in echelon form.

Now use Algorithm 10.5B to further reduce A to row canonical form. Specifically, multiply R_3 by $-\frac{1}{2}$ so the pivot entry $a_{35} = 1$, and then use $a_{35} = 1$ as a pivot to obtain zeros above it by the operations "Add $-6R_3$ to R_2" and "Add $-2R_3$ to R_1". This yields:

$$A \sim \begin{bmatrix} 1 & 2 & -3 & 1 & 2 \\ 0 & 0 & 2 & 4 & 6 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 1 & 2 & -3 & 1 & 0 \\ 0 & 0 & 2 & 4 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Multiply R_2 by $\frac{1}{2}$ so the pivot entry $a_{23} = 1$, and then use $a_{23} = 1$ as a pivot to obtain 0 above it by the operation "Add $3R_1$ to R_1". This yields:

$$A \sim \begin{bmatrix} 1 & 2 & -3 & 1 & 0 \\ 0 & 0 & 1 & 2 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 1 & 2 & 0 & 7 & 0 \\ 0 & 0 & 1 & 2 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

The last matrix is the row canonical form of A.

Algorithms 10.5A and 10.5B show that any matrix is row equivalent to at least one matrix in row canonical form. Actually, one proves in a course in linear algebra that such a matrix is unique. That is:

Theorem 5.6: Any matrix A is row equivalent to a unique matrix in row canonical form (called the *row canonical form* of A).

Matrix Solution of a System of Linear Equations

Consider a system S of linear equations or, equivalently, a matrix equation $AX = B$ with augmented matrix $M = [A, B]$. The system is solved by applying the above Gaussian elimination algorithm to M as follows.

Part A (*Reduction*): Reduce the augmented matrix M to echelon form. If a row of the form $(0, 0, \ldots, 0, b)$, with $b \neq 0$, appears, then *stop*. The system does not have a solution.

Part B (*Back-Substitution*): Further reduce the augmented matrix M to its row canonical form.

The unique solution of the system or, when the solution is not unique, the free variable form of the solution is easily obtained from the row canonical form of M.

The following example applies the above algorithm to a system S with a unique solution. The cases where S has no solution and where S has an infinite number of solutions are shown in Problems 5.32 and 5.31, respectively.

EXAMPLE 5.13 Solve the system:

$$\begin{aligned} x + 2y + z &= 3 \\ 2x + 5y - z &= -4 \\ 3x - 2y - z &= 5 \end{aligned}$$

Reduce its augmented matrix M to echelon form and then to row canonical form as follows:

$$M = \begin{bmatrix} 1 & 2 & 1 & 3 \\ 2 & 5 & -1 & -4 \\ 3 & -2 & -1 & 5 \end{bmatrix} \sim \begin{bmatrix} 1 & 2 & 1 & 3 \\ 0 & 1 & -3 & -10 \\ 0 & -8 & -4 & -4 \end{bmatrix} \sim \begin{bmatrix} 1 & 2 & 1 & 3 \\ 0 & 1 & -3 & -10 \\ 0 & 0 & -28 & -84 \end{bmatrix}$$

$$\sim \begin{bmatrix} 1 & 2 & 1 & 3 \\ 0 & 1 & -3 & -10 \\ 0 & 0 & 1 & 3 \end{bmatrix} \sim \begin{bmatrix} 1 & 2 & 0 & 0 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 3 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 0 & 2 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 3 \end{bmatrix}$$

Thus the system has the unique solution $x = 2, y = -1, z = 3$ or, equivalently, the vector $u = (2, -1, 3)$. We note that the echelon form of M already indicated that the solution was unique since it corresponded to a triangular system.

Inverse of an $n \times n$ Matrix

Consider an arbitrary 3×3 matrix $A = [a_{ij}]$. Finding $A^{-1} = [x_{ij}]$ reduces to finding the solution of three 3×3 systems of linear equations. The augmented matrices of these three systems follow:

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} & 1 \\ a_{21} & a_{22} & a_{23} & 0 \\ a_{31} & a_{32} & a_{33} & 0 \end{bmatrix}, \quad \begin{bmatrix} a_{11} & a_{12} & a_{13} & 0 \\ a_{21} & a_{22} & a_{23} & 1 \\ a_{31} & a_{32} & a_{33} & 0 \end{bmatrix}, \quad \begin{bmatrix} a_{11} & a_{12} & a_{13} & 0 \\ a_{21} & a_{22} & a_{23} & 0 \\ a_{31} & a_{32} & a_{33} & 1 \end{bmatrix}.$$

Note that the original matrix A is the coefficient matrix of all three systems. Also note that the three columns of constants form the identity matrix I. These three systems can be solved simultaneously by the following algorithm, which holds for any $n \times n$ matrix.

Algorithm 5.10C: Find the inverse of an $n \times n$ matrix A.

Step 1. Form the $n \times 2n$ matrix $M = [A, I]$; that is, A is in the left half of M and the identity matrix I is in the right half of M.

Step 2. Row reduce M to an echelon form. If the process generates a zero row in the A-half of M, then *stop* (A has no inverse). Otherwise the A-half is now in triangular form.

Step 3. Further row reduce M to the row canonical form

$$M \sim [I, B]$$

where I has replaced A in the left half of M.

Step 4. Set $A^{-1} = B$, where B is the matrix that is now in the right half of M.

EXAMPLE 5.14 Find the inverse of

$$A = \begin{bmatrix} 1 & 0 & 2 \\ 2 & -1 & 3 \\ 4 & 1 & 8 \end{bmatrix}$$

Form the matrix $M = (A, I)$ and reduce M to echelon form:

$$M = \left[\begin{array}{ccc|ccc} 1 & 0 & 2 & 1 & 0 & 0 \\ 2 & -1 & 3 & 0 & 1 & 0 \\ 4 & 1 & 8 & 0 & 0 & 1 \end{array}\right] \sim \left[\begin{array}{ccc|ccc} 1 & 0 & 2 & 1 & 0 & 0 \\ 0 & -1 & -1 & -2 & 1 & 0 \\ 0 & 1 & 0 & -4 & 0 & 1 \end{array}\right] \sim \left[\begin{array}{ccc|ccc} 1 & 0 & 2 & 1 & 0 & 0 \\ 0 & -1 & -1 & -2 & 1 & 0 \\ 0 & 0 & -1 & -6 & 1 & 1 \end{array}\right]$$

In echelon form, the left half of M is in triangular form; hence A is invertible. Further row reduce M to row canonical form:

$$M \sim \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & -11 & 2 & 2 \\ 0 & -1 & 0 & 4 & 0 & -1 \\ 0 & 0 & 1 & 6 & -1 & -1 \end{array}\right] \sim \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & -11 & 2 & 2 \\ 0 & 1 & 0 & -4 & 0 & 1 \\ 0 & 0 & 1 & 6 & -1 & -1 \end{array}\right]$$

The identity matrix is in the left half of the final matrix; hence the right half is A^{-1}. In other words,

$$A^{-1} = \begin{bmatrix} -11 & 2 & 2 \\ -4 & 0 & 1 \\ 6 & -1 & -1 \end{bmatrix}$$

5.11 BOOLEAN (ZERO–ONE) MATRICES

The *binary digits* or *bits* are the symbols 0 and 1. Consider the following operations on these digits:

$+$	0	1
0	0	1
1	1	1

$\times$	0	1
0	0	0
1	0	1

Viewing these bits as logical values (0 representing FALSE and 1 representing TRUE), the above operations correspond, respectively, to the logical operations of OR ($\vee$) and AND ($\wedge$); that is,

$\vee$	F	T
F	F	T
T	T	T

$\wedge$	F	T
F	F	F
T	F	T

(The above operations on 0 and 1 are called *Boolean operations* since they also correspond to the operations of a Boolean algebra discussed in Chapter 15.)

Now let $A = [a_{ij}]$ be a matrix whose entries are the bits 0 and 1 subject to the above Boolean operations. Then A is called a *Boolean matrix*. The *Boolean product* of two such matrices is the usual product except that now we use the Boolean operations of addition and multiplication. For example, if

$$A = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \text{ and } B = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}, \qquad \text{then} \qquad AB = \begin{bmatrix} 0+0 & 1+1 \\ 0+0 & 1+0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}$$

One can easily show that if A and B are Boolean matrices, then the Boolean product AB can be obtained by finding the usual product of A and B and then replacing any nonzero digit by 1.

Solved Problems

VECTORS

5.1. Let $u = (2, -7, 1)$, $v = (-3, 0, 4)$ and $w = (0, 5, -8)$. Find:
(a) $u + v$; (b) $v + w$; (c) $-3u$; (d) $-w$.

(a) Add corresponding components:

$$u + v = (2, -7, 1) + (-3, 0, 4) = (2 - 3, -7 + 0, 1 + 4) = (-1, -7, 5)$$

(b) Add corresponding components:

$$v + w = (-3, 0, 4) + (0, 5, -8) = (-3 + 0, 0 + 5, 4 - 8) = (-3, 5, -4)$$

(c) Multiply each component of u by the scalar -3:

$$-3u = -3(2, -7, 1) = (-6, 21, -3)$$

(d) Change the sign of each component or, equivalently, multiply each component by -1;

$$-w = -(0, 5, -8) = (0, -5, 8)$$

5.2. Let u, v, and w be the vectors in Problem 5.1. Find: (*a*) $3u - 4v$; (*b*) $2u + 3v - 5w$.

First perform the scalar multiplication and then the vector addition.

(*a*) $3u - 4v = 3(2, -7, 1) - 4(-3, 0, 4) = (6, -21, 3) + (12, 0, -16) = (18, -21, -13)$.

(*b*) $2u + 3v - 6w =$
$2(2, -7, 1) + 3(-3, 0, 4) - 5(0, 5, -8) = (4, -14, 2) + (-9, 0, 12) + 0, -25, 40) = (-5, -39, 54)$.

5.3. Let u, v, and w be the vectors in Problem 5.1. Find: (*a*) $u \cdot v$; (*b*) $u \cdot w$; (*c*) $v \cdot w$.

Multiply corresponding components and then add:

(*a*) $u \cdot v = 2(-3) - 7(0) + 1(4) = -6 + 0 + 4 = -2$.

(*b*) $u \cdot w = 2(0) - 7(5) + 1(-8) = 0 - 35 - 8 = -43$.

(*c*) $v \cdot w = -3(0) + 0(5) + 4(-8) = 0 + 0 - 32 = -32$.

5.4. Find $\|u\|$ where: (*a*) $u = (3, -12, -4)$; (*b*) $u = (2, -3, 8, -7)$.

First find $\|u\|^2 = u \cdot u$ by squaring the components and adding. Then $\|u\| = \sqrt{\|u\|^2}$.

(*a*) $\|u\|^2 = (3)^2 + (-12)^2 + (-4)^2 = 9 + 144 + 16 = 169$.

Hence $\|u\| = \sqrt{169} = 13$.

(*b*) $\|u\|^2 = 4 + 9 + 64 + 49 = 126$. Hence $\|u\| = \sqrt{126}$.

5.5. Find x and y if $x(1, 1) + y(2, -1) = 1, 4)$.

First multiply by the scalars x and y and then add:

$$x(1, 1) + y(2, -1) \quad = \quad (x, x) + (2y, -y) \quad = \quad (x + 2y, x - y) \quad = \quad (1, 4)$$

Two vectors are equal only when their corresponding components are equal; hence set the corresponding components equal to each other to obtain $x + 2y = 1$ and $x - y = 4$. Finally, solve the system of equations to obtain $x = 3$ and $y = -1$.

5.6. Suppose $u = \begin{bmatrix} 5 \\ 3 \\ -4 \end{bmatrix}, v = \begin{bmatrix} -1 \\ 5 \\ 2 \end{bmatrix}, w = \begin{bmatrix} 3 \\ -1 \\ -2 \end{bmatrix}$. Find: (*a*) $5u - 2v$; (*b*) $-2u + 4v - 3w$.

(*a*) $5u - 2v = 5\begin{bmatrix} 5 \\ 3 \\ -4 \end{bmatrix} - 2\begin{bmatrix} -1 \\ 5 \\ 2 \end{bmatrix} = \begin{bmatrix} 25 \\ 15 \\ -20 \end{bmatrix} + \begin{bmatrix} 2 \\ -10 \\ 4 \end{bmatrix} = \begin{bmatrix} 27 \\ 5 \\ -24 \end{bmatrix}$.

(*b*) $-2u + 4v - 3w = \begin{bmatrix} -10 \\ -6 \\ 8 \end{bmatrix} + \begin{bmatrix} -4 \\ 20 \\ 8 \end{bmatrix} + \begin{bmatrix} -9 \\ 3 \\ 6 \end{bmatrix} = \begin{bmatrix} -23 \\ 17 \\ 22 \end{bmatrix}$.

MATRIX ADDITION AND SCALAR MULTIPLICATION

5.7. Given $A = \begin{bmatrix} 1 & 2 & -3 \\ 4 & -5 & 6 \end{bmatrix}$ and $B = \begin{bmatrix} 1 & -1 & 2 \\ 0 & 3 & -5 \end{bmatrix}$. Find: (*a*) $A + B$; (*b*) $3A$ and $-4B$.

(*a*) Add corresponding elements:

$$A + B = \begin{bmatrix} 1 + 1 & 2 + (-1) & -3 + 2 \\ 4 + 0 & -5 + 3 & 6 + (-5) \end{bmatrix} = \begin{bmatrix} 2 & 1 & -1 \\ 4 & -2 & 1 \end{bmatrix}$$

(*b*) Multiply each entry by the given scalar:

$$3A = \begin{bmatrix} 3(1) & 3(2) & 3(-3) \\ 3(4) & 3(-5) & 3(6) \end{bmatrix} = \begin{bmatrix} 3 & 6 & -9 \\ 12 & -15 & 18 \end{bmatrix}$$

$$-4B = \begin{bmatrix} -4(1) & -4(-1) & -4(2) \\ -4(0) & -4(3) & -4(-5) \end{bmatrix} = \begin{bmatrix} -4 & 4 & -8 \\ 0 & -12 & 20 \end{bmatrix}$$

5.8. Find $2A - 3B$, where $A = \begin{bmatrix} 1 & -2 & 3 \\ 4 & 5 & -6 \end{bmatrix}$ and $B = \begin{bmatrix} 3 & 0 & 2 \\ -7 & 1 & 8 \end{bmatrix}$.

First perform the scalar multiplications, and then a matrix addition:

$$2A - 3B = \begin{bmatrix} 2 & -4 & 6 \\ 8 & 10 & -12 \end{bmatrix} + \begin{bmatrix} -9 & 0 & -6 \\ 21 & -3 & -24 \end{bmatrix} = \begin{bmatrix} -7 & -4 & 0 \\ 29 & 7 & -36 \end{bmatrix}$$

(Note that we multiply B by -3 and then add, rather than multiplying B by 3 and subtracting. This usually avoids errors.)

5.9. Find x, y, z, t, where $3\begin{bmatrix} x & y \\ z & t \end{bmatrix} = \begin{bmatrix} x & 6 \\ -1 & 2t \end{bmatrix} + \begin{bmatrix} 4 & x+y \\ z+t & 3 \end{bmatrix}$.

First write each side as a single matrix:

$$\begin{bmatrix} 3x & 3y \\ 3z & 3t \end{bmatrix} = \begin{bmatrix} x+4 & x+y+6 \\ z+t-1 & 2t+3 \end{bmatrix}$$

Set corresponding entries equal to each other to obtain the system of four equations.

$$\begin{aligned} 3x &= x+4 \\ 3y &= x+y+6 \\ 3z &= z+t-1 \\ 3t &= 2t+3 \end{aligned} \quad \text{or} \quad \begin{aligned} 2x &= 4 \\ 2y &= 6+x \\ 2z &= t-1 \\ t &= 3 \end{aligned}$$

The solution is $x = 2$, $y = 4$, $z = 1$, $t = 3$.

5.10. Prove Theorem 5.1(v): $k(A + B) = kA + kB$.

Let $A = [a_{ij}]$ and $B = [b_{ij}]$. Then the ij entry of $A + B$ is $a_{ij} + b_{ij}$. Hence $k(a_{ij} + b_{ij})$ is the ij entry of $k(A + B)$. On the other hand, the ij entries of kA and kB are ka_{ij} and kb_{ij}, respectively. Thus $ka_{ij} + kb_{ij}$ is the ij entry. However, for scalars, $k(a_{ij} + b_{ij}) = ka_{ij} + kb_{ij}$. Thus $k(A + B)$ and $kA + kB$ have the same ij entries. Therefore, $k(A + B) = kA + kB$.

MATRIX MULTIPLICATION

5.11. Calculate: (*a*) $[3, -2, 5]\begin{bmatrix} 6 \\ 1 \\ -4 \end{bmatrix}$; (*b*) $[2, -1, 7, 4]\begin{bmatrix} 5 \\ -3 \\ -6 \\ 9 \end{bmatrix}$.

Multiply corresponding entries and then add:

(*a*) $[3, -2, 5]\begin{bmatrix} 6 \\ 1 \\ -4 \end{bmatrix} = 3(6) - 2(1) + 5(-4) = 18 - 2 - 20 = -4.$

(*b*) $[2, -1, 7, 4]\begin{bmatrix} 5 \\ -3 \\ -6 \\ 9 \end{bmatrix} = 10 + 3 - 42 + 36 = 7.$

5.12. Let $(r \times s)$ denote an $r \times s$ matrix. Find the sizes of those matrix products which are defined:

(*a*) $(2 \times 3)(3 \times 4)$ (*c*) $(1 \times 2)(3 \times 1)$ (*e*) $(4 \times 4)(3 \times 3)$

(*b*) $(4 \times 1)(1 \times 2)$ (*d*) $(5 \times 2)(2 \times 3)$ (*f*) $(2 \times 2)(2 \times 4)$

In each case the product is defined if the inner numbers are equal, and then the product will have the size of the outer numbers in the given order:

(*a*) 2×4 (*c*) Not defined (*e*) Not defined

(*b*) 4×2 (*d*) 5×3 (*f*) 2×4

5.13. Let $A = \begin{bmatrix} 1 & 3 \\ 2 & -1 \end{bmatrix}$ and $B = \begin{bmatrix} 2 & 0 & -4 \\ 3 & -2 & 6 \end{bmatrix}$. Find: (*a*) AB; (*b*) BA.

(*a*) Since A is 2×2 and B is 2×3, the product AB is defined and is a 2×3 matrix. To obtain the first row of AB, multiply the first row $[1, 3]$ of A by the columns $\begin{bmatrix} 2 \\ 3 \end{bmatrix}$, $\begin{bmatrix} 0 \\ -2 \end{bmatrix}$, $\begin{bmatrix} -4 \\ 6 \end{bmatrix}$ of B, respectively:

$$\begin{bmatrix} 1 & 3 \\ 2 & -1 \end{bmatrix}\begin{bmatrix} 2 & 0 & -4 \\ 3 & -2 & 6 \end{bmatrix} = \begin{bmatrix} 1(2)+3(3) & 1(0)+3(-1) & 1(-4)+3(6) \\ & & \end{bmatrix}$$

$$= \begin{bmatrix} 2+9 & 0-6 & -4+18 \\ & & \end{bmatrix} = \begin{bmatrix} 11 & -6 & 14 \\ & & \end{bmatrix}$$

To obtain the entries in the second row of AB, multiply the second row $[2, -1]$ of A by the columns of B, respectively:

$$\begin{bmatrix} 1 & 3 \\ 2 & -1 \end{bmatrix}\begin{bmatrix} 2 & 0 & -4 \\ 3 & -2 & 6 \end{bmatrix} = \begin{bmatrix} 11 & -6 & 14 \\ 4-3 & 0+2 & -8-6 \end{bmatrix}$$

Thus

$$AB = \begin{bmatrix} 11 & -6 & 14 \\ 1 & 2 & -14 \end{bmatrix}$$

(*b*) Note that B is 2×3 and A is 2×2. Since the inner numbers, 3 and 2, are not equal, the product BA is not defined.

5.14. Compute: (*a*) $\begin{bmatrix} 1 & 6 \\ -3 & 5 \end{bmatrix}\begin{bmatrix} 4 & 0 \\ 2 & -1 \end{bmatrix}$; (*b*) $\begin{bmatrix} 1 & 6 \\ -3 & 5 \end{bmatrix}\begin{bmatrix} 2 \\ -7 \end{bmatrix}$; (*c*) $\begin{bmatrix} 1 \\ -6 \end{bmatrix}\begin{bmatrix} 1 & 6 \\ -3 & 5 \end{bmatrix}$;

(*d*) $\begin{bmatrix} 1 \\ 6 \end{bmatrix}[3, 2]$; (*e*) $[2, -1]\begin{bmatrix} 1 \\ -6 \end{bmatrix}$.

(*a*) The first factor is 2×2 and the second is 2×2, so the product is defined and is a 2×2 matrix:

$$\begin{bmatrix} 1 & 6 \\ -3 & 5 \end{bmatrix}\begin{bmatrix} 4 & 0 \\ 2 & -1 \end{bmatrix} = \begin{bmatrix} 4+12 & 0+12 \\ -12+10 & 0-5 \end{bmatrix} = \begin{bmatrix} 16 & -6 \\ -2 & -5 \end{bmatrix}$$

(*b*) The first factor is 2×2 and the second is 2×1, so the product is defined and is a 2×1 matrix:

$$\begin{bmatrix} 1 & 6 \\ -3 & 5 \end{bmatrix}\begin{bmatrix} 2 \\ -7 \end{bmatrix} = \begin{bmatrix} 2-42 \\ -6-35 \end{bmatrix} = \begin{bmatrix} -40 \\ -41 \end{bmatrix}$$

(*c*) Now the first factor is 2×1 and the second is 2×2. Since the inner numbers 1 and 2 are different, the product is not defined.

(*d*) Here the first factor is 2×1 and the second is 1×2, so the product is defined and is a 2×2 matrix:

$$\begin{bmatrix} 1 \\ 6 \end{bmatrix}[3, 2] = \begin{bmatrix} 1(3) & 1(2) \\ 6(3) & 6(2) \end{bmatrix} = \begin{bmatrix} 3 & 2 \\ 18 & 12 \end{bmatrix}$$

(*e*) The first factor is 1×2 and the second is 2×1, so the product is defined and is a 1×1 matrix which we typically write as a scalar:

$$[2, -1]\begin{bmatrix} 1 \\ -6 \end{bmatrix} = 2(1) - 1(-6) = 2 + 6 = 8$$

5.15. Prove Theorem 5.2(i): $(AB)C = A(BC)$.

Let $A = [a_{ij}]$, $B = [b_{jk}]$, and $C = [c_{kl}]$. Furthermore, let $AB = S = [s_{ik}]$ and $BC = T = [t_{jl}]$.

Then

$$s_{ik} = a_{i1}b_{1k} + a_{i2}b_{2k} + \cdots + a_{im}b_{mk} = \sum_{j=1}^{m} a_{ij}b_{jk}$$

$$t_{jl} = b_{j1}c_{sl} + b_{j2}c_{2l} + \cdots + b_{jn}c_{nl} = \sum_{k=l}^{n} b_{jk}c_{kl}$$

Now, multiplying S by C, i.e., (AB) by C, the element in the ith row and lth column of the matrix $(AB)C$ is

$$s_{i1}c_{1l} + s_{i2}c_{2l} + \cdots + s_{in}c_{nl} = \sum_{k=1}^{n} s_{ik}c_{kl} = \sum_{k=1}^{n}\sum_{j=1}^{m}(a_{ij}b_{jk})c_{kl}$$

On the other hand, multiplying A by T, i.e., A by BC, the element in the ith row and lth column of the matrix $A(BC)$ is

$$a_{i1}t_{1l} + a_{i2}t_{2l} + \cdots + a_{im}t_{ml} = \sum_{j=1}^{m} a_{ij}t_{jl} = \sum_{k=1}^{m}\sum_{j=1}^{n} a_{ij}(b_{jk}c_{kl})$$

Since the above sums are equal, the theorem is proven.

TRANSPOSE

5.16. Find the transpose of each matrix:

$$A = \begin{bmatrix} 1 & -2 & 3 \\ 7 & 8 & -9 \end{bmatrix}; \qquad B = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 4 & 5 \\ 3 & 5 & 6 \end{bmatrix}; \qquad C = [1, -3, 5, -7]; \qquad D = \begin{bmatrix} 2 \\ -4 \\ 6 \end{bmatrix}.$$

Rewrite the rows of each matrix as columns to obtain the transposes of the matrices:

$$A^T = \begin{bmatrix} 1 & 7 \\ -2 & 8 \\ 3 & -9 \end{bmatrix}, \qquad B^T = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 4 & 5 \\ 3 & 5 & 6 \end{bmatrix}, \qquad C^T = \begin{bmatrix} 1 \\ -3 \\ 5 \\ -7 \end{bmatrix}, \qquad D^T = [2, -4, 6]$$

(Note that $B^T = B$; such a matrix is said to be *symmetric*. Note also that the transpose of the row vector C is a column vector, and the transpose of the column vector D is a row vector.)

5.17. Let $A = \begin{bmatrix} 1 & 2 & 0 \\ 3 & -1 & 4 \end{bmatrix}$. Find (*a*) AA^T; (*b*) A^TA.

To obtain A^T, rewrite the rows of A as columns: $A^T = \begin{bmatrix} 1 & 3 \\ 2 & -1 \\ 0 & 4 \end{bmatrix}$. Then

(*a*) $$AA^T = \begin{bmatrix} 1 & 2 & 0 \\ 3 & -1 & 4 \end{bmatrix}\begin{bmatrix} 1 & 3 \\ 2 & -1 \\ 0 & 4 \end{bmatrix} = \begin{bmatrix} 1+4+0 & 3-2+0 \\ 3-2+0 & 9+1+16 \end{bmatrix} = \begin{bmatrix} 5 & 1 \\ 1 & 26 \end{bmatrix}.$$

$$(b)\quad A^TA=\begin{bmatrix}1&3\\2&-1\\0&4\end{bmatrix}\begin{bmatrix}1&2&0\\3&-1&4\end{bmatrix}=\begin{bmatrix}1+9&2-3&0+12\\2-3&4+1&0-4\\0+12&0-4&0+16\end{bmatrix}=\begin{bmatrix}10&-1&12\\-1&5&-4\\12&-4&16\end{bmatrix}.$$

5.18. Prove Theorem 5.3(iii): $(AB)^T=B^TA^T$.

Suppose $A=[a_{ik}]$ and $B=[b_{kj}]$. Then the ij entry of AB is

$$a_{i1}b_{1j}+a_{i2}b_{2j}+\cdots+a_{im}b_{mj} \tag{1}$$

Thus (1) is the ji entry [reverse order] of $(AB)^T$.

On the other hand, column j of B becomes row j of B^T, and row i of A becomes column i of A^T. Consequently, the ji-entry of B^TA^T is

$$[b_{1j},b_{2j},\cdots,b_{mj}]\begin{bmatrix}a_{i1}\\a_{i2}\\\cdots\\a_{im}\end{bmatrix}=b_{ij}a_{i1}+b_{2j}a_{i2}+\cdots+b_{mj}a_{im}$$

Thus, $(AB)^T=B^TA^T$, since corresponding entries are equal.

SQUARE MATRICES

5.19. Find the diagonal of each of the following matrices:

$$(a)\ A=\begin{bmatrix}1&3&6\\2&-5&8\\4&-2&7\end{bmatrix};\qquad (b)\ B=\begin{bmatrix}t-2&3\\-4&t+5\end{bmatrix};\qquad (c)\ C=\begin{bmatrix}1&2&-3\\4&-5&6\end{bmatrix}.$$

(*a*) The diagonal consists of the elements from the upper left corner to the lower right corner of the matrix, that is, the elements a_{11}, a_{22}, a_{33}. Thus the diagonal of A consists of the scalars 1, -5, and 7.

(*b*) The diagonal consists of the pair $[t-2,t+5]$.

(*c*) The diagonal is defined only for square matrices.

5.20. Let $A=\begin{bmatrix}1&2\\4&-3\end{bmatrix}$. Find: (*a*) A^2; (*b*) A^3.

$$(a)\quad A^2=AA=\begin{bmatrix}1&2\\4&-3\end{bmatrix}\begin{bmatrix}1&2\\4&-3\end{bmatrix}=\begin{bmatrix}1+8&2-6\\4-12&8+9\end{bmatrix}=\begin{bmatrix}9&-4\\-8&17\end{bmatrix}.$$

$$(b)\quad A^3=AA^2=\begin{bmatrix}1&2\\4&-3\end{bmatrix}\begin{bmatrix}9&-4\\-8&17\end{bmatrix}=\begin{bmatrix}9-16&-4+34\\36+24&-16-51\end{bmatrix}=\begin{bmatrix}-7&30\\60&-67\end{bmatrix}.$$

5.21. Let $f(x)=2x^3-4x+5$ and $g(x)=x^2+2x-11$. For the matrix A in Problem 5.20, find: (*a*) $f(A)$; (*b*) $g(A)$.

(*a*) Compute $f(A)$ by first substituting A for x and $5I$ for the constant term 5 in $f(x)=2x^3-4x+5$:

$$f(A)=2A^3-4A+5I=2\begin{bmatrix}-7&30\\60&-67\end{bmatrix}-4\begin{bmatrix}1&2\\4&-3\end{bmatrix}+5\begin{bmatrix}1&0\\0&1\end{bmatrix}$$

Then multiply each matrix by its respective scalar:

$$f(A) = \begin{bmatrix} -14 & 60 \\ 120 & -134 \end{bmatrix} + \begin{bmatrix} -4 & -8 \\ -16 & 12 \end{bmatrix} + \begin{bmatrix} 5 & 0 \\ 0 & 5 \end{bmatrix}$$

Lastly, add the corresponding elements in the matrices:

$$f(A) = \begin{bmatrix} -14-4+5 & 60-8+0 \\ 120-16+0 & -134+12+5 \end{bmatrix} = \begin{bmatrix} -13 & 52 \\ 104 & -117 \end{bmatrix}$$

(*b*) Compute $g(A)$ by first substituting A for x and $11I$ for the constant term 11 in $g(x) = x^2 + 2x - 11$:

$$g(A) = A^2 + 2A - 11I = \begin{bmatrix} 9 & -4 \\ -8 & 17 \end{bmatrix} + 2\begin{bmatrix} 1 & 2 \\ 4 & -3 \end{bmatrix} - 11\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$
$$= \begin{bmatrix} 9 & -4 \\ -8 & 17 \end{bmatrix} + \begin{bmatrix} 2 & 4 \\ 8 & -6 \end{bmatrix} + \begin{bmatrix} -11 & 0 \\ 0 & -11 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

(Since $g(A) = 0$, the matrix A is a zero of the polynomial $g(x)$.)

DETERMINANTS AND INVERSES

5.22. Compute the determinant of each matrix:

(*a*) $\begin{bmatrix} 4 & 5 \\ -3 & -2 \end{bmatrix}$; (*b*) $\begin{bmatrix} -2 & 7 \\ 0 & 6 \end{bmatrix}$; (*c*) $\begin{bmatrix} a-b & b \\ b & a+b \end{bmatrix}$; (*d*) $\begin{bmatrix} a-b & a \\ a & a+b \end{bmatrix}$.

Use the formula $\begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc$ to obtain:

(*a*) $\begin{vmatrix} 4 & 5 \\ -3 & -2 \end{vmatrix} = 4(-2) - 5(-3) = -8 + 15 = 7.$

(*b*) $\begin{vmatrix} -2 & 7 \\ 0 & 6 \end{vmatrix} = -2(6) - 7(0) = -12 + 0 = -12.$

(*c*) $\begin{vmatrix} a-b & b \\ b & a+b \end{vmatrix} = (a-b)(a+b) - b^2 = a^2 - b^2 - b^2 = a^2 - 2b^2.$

(*d*) $\begin{vmatrix} a-b & a \\ a & a+b \end{vmatrix} = (a-b)(a+b) - a^2 = a^2 - b^2 - a^2 = -b^2.$

5.23. Find the determinant of each matrix:

(*a*) $\begin{bmatrix} 1 & 2 & 3 \\ 4 & -2 & 3 \\ 0 & 5 & -1 \end{bmatrix}$; (*b*) $\begin{bmatrix} 4 & -1 & -2 \\ 0 & 2 & -3 \\ 5 & 2 & 1 \end{bmatrix}$; (*c*) $\begin{bmatrix} 2 & -3 & 4 \\ 1 & 2 & -3 \\ -1 & -2 & 5 \end{bmatrix}$.

(*Hint*: Use the diagram in Section 5.9)

(*a*) $\begin{vmatrix} 1 & 2 & 3 \\ 4 & -2 & 3 \\ 0 & 5 & -1 \end{vmatrix} = 2 + 0 + 60 - 0 - 15 + 8 = 55.$

(*b*) $\begin{vmatrix} 4 & -1 & -2 \\ 0 & 2 & -3 \\ 5 & 2 & 1 \end{vmatrix} = 8 + 15 + 0 + 20 + 24 + 0 = 67.$

(*c*) $\begin{vmatrix} 2 & -3 & 4 \\ 1 & 2 & -3 \\ -1 & -2 & 5 \end{vmatrix} = 20 - 9 - 8 + 8 - 12 + 15 = 14.$

5.24. Find the inverse, if possible, of each matrix:

$$(a)\ A = \begin{bmatrix} 5 & 3 \\ 4 & 2 \end{bmatrix}; \qquad (b)\ B = \begin{bmatrix} 2 & -3 \\ 1 & 3 \end{bmatrix}; \qquad (c)\ C = \begin{bmatrix} -2 & 6 \\ 3 & -9 \end{bmatrix}.$$

For a 2×2 matrix, use the formula developed in Section 5.9.

(*a*) First find $|A| = 5(2) - 3(4) = 10 - 12 = -2$. Next, interchange the diagonal elements, take the negatives of the nondiagonal elements, and multiply by $1/|A|$:

$$A^{-1} = -\frac{1}{2}\begin{bmatrix} 2 & -3 \\ -4 & 5 \end{bmatrix} = \begin{bmatrix} -1 & \frac{3}{2} \\ 2 & -\frac{5}{2} \end{bmatrix}$$

(*b*) First find $|B| = 2(3) - (-3)(1) = 6 + 3 = 9$. Next, interchange the diagonal elements, take the negatives of the nondiagonal elements, and multiply by $1/|B|$:

$$B^{-1} = \tfrac{1}{9}\begin{bmatrix} 3 & 3 \\ -1 & 2 \end{bmatrix} = \begin{bmatrix} \frac{1}{3} & \frac{1}{3} \\ -\frac{1}{9} & \frac{2}{9} \end{bmatrix}$$

(*c*) First find $|C| = -2(-9) - 6(3) = 18 - 18 = 0$. Since $|C| = 0$, C has no inverse

5.25. Find the inverse of $A = \begin{bmatrix} 1 & -2 & 2 \\ 2 & -3 & 6 \\ 1 & 1 & 7 \end{bmatrix}$.

Form the matrix $M = (A, I)$ and row reduce M to echelon form:

$$M = \left[\begin{array}{ccc|ccc} 1 & -2 & 2 & 1 & 0 & 0 \\ 2 & -3 & 6 & 0 & 1 & 0 \\ 1 & 1 & 7 & 0 & 0 & 1 \end{array}\right] \sim \left[\begin{array}{ccc|ccc} 1 & -2 & 2 & 1 & 0 & 0 \\ 0 & 1 & 2 & -2 & 1 & 0 \\ 0 & 3 & 5 & -1 & 0 & 1 \end{array}\right] \sim \left[\begin{array}{ccc|ccc} 1 & -2 & 2 & 1 & 0 & 0 \\ 0 & 1 & 2 & -2 & 1 & 0 \\ 0 & 0 & -1 & 5 & -3 & 1 \end{array}\right]$$

In echelon form, the left half of M is in triangular form; hence A has an inverse. Further reduce M to row canonical form:

$$M \sim \left[\begin{array}{ccc|ccc} 1 & -2 & 0 & 11 & -6 & 2 \\ 0 & 1 & 0 & 8 & -5 & 2 \\ 0 & 0 & 1 & -5 & 3 & -1 \end{array}\right] \sim \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 27 & -16 & 1 \\ 0 & 1 & 0 & 8 & -5 & 2 \\ 0 & 0 & 1 & -5 & 3 & -1 \end{array}\right]$$

The final matrix has the form $[I, A^{-1}]$; that is, A^{-1} is the right half of the last matrix. Thus

$$A^{-1} = \begin{bmatrix} 27 & -16 & 6 \\ 8 & -5 & 2 \\ -5 & 3 & -1 \end{bmatrix}$$

5.26. Find the inverse of $B = \begin{bmatrix} 1 & 3 & -4 \\ 1 & 5 & -1 \\ 3 & 13 & -6 \end{bmatrix}$.

Form the matrix $M = [B, I]$ and row reduce M to echelon form:

$$M = \left[\begin{array}{ccc|ccc} 1 & 3 & -4 & 1 & 0 & 0 \\ 1 & 5 & -1 & 0 & 1 & 0 \\ 3 & 13 & -6 & 0 & 0 & 1 \end{array}\right] \sim \left[\begin{array}{ccc|ccc} 1 & 3 & -4 & 1 & 0 & 0 \\ 0 & 2 & 3 & -1 & 1 & 0 \\ 0 & 4 & 6 & -3 & 0 & 1 \end{array}\right] \sim \left[\begin{array}{ccc|ccc} 1 & 3 & -4 & 1 & 0 & 0 \\ 0 & 2 & 3 & -1 & 1 & 0 \\ 0 & 0 & 0 & -1 & -2 & 1 \end{array}\right]$$

In echelon form, M has a zero row in its left half; that is, B is not row reducible to triangular form. Accordingly, B has no inverse.

5.27. Let A be an invertible matrix with inverse B. In other words, $AB = BA = I$. Show that the inverse matrix B is unique.

Let B_1 and B_2 be any two inverses of matrix A. In other words, let $AB_1 = B_1A = I$ and $AB_2 = B_2A = I$, then $B_1 = B_1I = B_1(AB_2) = (B_1A)B_2 = IB_2 = B_2$.

5.28. Suppose A and B are invertible matrices of the same order. Show that AB is invertible and that $(AB)^{-1} = B^{-1}A^{-1}$.

We have

$$(AB)(B^{-1}A^{-1}) = A(BB^{-1})A^{-1} = AIA^{-1} = AA^{-1} = I$$

and

$$(B^{-1}A^{-1}(AB) = B^{-1}(A^{-1}A)B = B^{-1}IB = B^{-1}B = I$$

Thus, $B^{-1}A^{-1}$ is the inverse of AB; that is $(AB)^{-1} = B^{-1}A^{-1}$.

ECHELON MATRICES, ROW REDUCTION, GAUSSIAN ELIMINATION

5.29. Interchange the rows in each matrix to obtain an echelon matrix:

$$(a)\ \begin{bmatrix} 0 & 1 & -3 & 4 & 6 \\ 4 & 0 & 2 & 5 & -3 \\ 0 & 0 & 7 & -2 & 8 \end{bmatrix}; \quad (b)\ \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 3 & 4 & 5 \\ 0 & 0 & 5 & -4 & 7 \end{bmatrix}; \quad (c)\ \begin{bmatrix} 0 & 2 & 2 & 2 & 2 \\ 0 & 3 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

(*a*) Interchange the first and second rows.

(*b*) Bring the zero row to the bottom of the matrix.

(*c*) No number of row interchange can produce an echelon matrix.

5.30. Row reduce the following matrix to echelon form:

$$A = \begin{bmatrix} 1 & 2 & -3 & 0 \\ 2 & 4 & -2 & 2 \\ 3 & 6 & -4 & 3 \end{bmatrix}$$

Use a_{11} as a pivot to obtain zeros below a_{11}; that is, apply the row operations "Add $-2R_1$ to R_2" and "Add $-3R_1$ to R_3". This yields the matrix

$$\begin{bmatrix} 1 & 2 & -3 & 0 \\ 0 & 0 & 4 & 2 \\ 0 & 0 & 5 & 3 \end{bmatrix}$$

Now use $a_{23} = 4$ as a pivot to obtain a zero below a_{23}; that is, apply the row operation "Add $-5R_2$ to $4R_3$" to obtain the matrix

$$\begin{bmatrix} 1 & 2 & -3 & 0 \\ 0 & 0 & 4 & 2 \\ 0 & 0 & 0 & 2 \end{bmatrix}$$

which is in echelon form.

5.31. Which of the following echelon matrices are in row canonical form?

$$\begin{bmatrix} 1 & 2 & -3 & 0 & 1 \\ 0 & 0 & 5 & 2 & -4 \\ 0 & 0 & 0 & 7 & 3 \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 & 7 & -5 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 & 5 & 0 & 2 \\ 0 & 1 & 2 & 0 & 4 \\ 0 & 0 & 0 & 1 & 7 \end{bmatrix}$$

The first matrix is not in row canonical form since, for example, two leading nonzero entries are 5 and 7, not 1. Also, there are nonzero entries above the leading nonzero entries 5 and 7. The second and third matrices are in row canonical form.

5.32. Reduce the following matrix to row canonical form:

$$A = \begin{bmatrix} 1 & -2 & 3 & 1 & 2 \\ 1 & 1 & 4 & -1 & 3 \\ 2 & 5 & 9 & -2 & 8 \end{bmatrix}$$

First reduce A to echelon form by applying the operations "Add $-R_1$ to R_2" and "Add $-2R_1$ to R_3," and then the operation "Add $-3R_2$ to R_3". These operations yield

$$A \sim \begin{bmatrix} 1 & -2 & 3 & 1 & 2 \\ 0 & 3 & 1 & -2 & 1 \\ 0 & 9 & 3 & -4 & 4 \end{bmatrix} \sim \begin{bmatrix} 1 & -2 & 3 & 1 & 2 \\ 0 & 3 & 1 & -2 & 1 \\ 0 & 0 & 0 & 2 & 1 \end{bmatrix}$$

Now use back-substitution on the echelon matrix to obtain the row canonical form of A. Specifically, first multiply R_3 by $\frac{1}{2}$ to obtain the pivot $a_{34} = 1$, and then apply the operations "Add $2R_3$ to R_2" and "Add $-R_3$ to R_1". These operations yield

$$A \sim \begin{bmatrix} 1 & -2 & 3 & 1 & 2 \\ 0 & 3 & 1 & -2 & 1 \\ 0 & 0 & 0 & 1 & \frac{1}{2} \end{bmatrix} \sim \begin{bmatrix} 1 & -2 & 3 & 0 & \frac{3}{2} \\ 0 & 3 & 1 & 0 & 2 \\ 0 & 0 & 0 & 1 & \frac{1}{2} \end{bmatrix}$$

Now multiply R_2 by $\frac{1}{3}$ making the pivot $a_{22} = 1$, and then apply the operation "Add $2R_2$ to R_1" We obtain

$$A \sim \begin{bmatrix} 1 & -2 & 3 & 0 & \frac{3}{2} \\ 0 & 1 & \frac{1}{3} & 0 & \frac{2}{3} \\ 0 & 0 & 0 & 1 & \frac{1}{2} \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & \frac{11}{3} & 0 & \frac{17}{6} \\ 0 & 1 & \frac{1}{3} & 0 & \frac{2}{3} \\ 0 & 0 & 0 & 1 & \frac{1}{2} \end{bmatrix}$$

Since $a_{11} = 1$, the last matrix is the desired row canonical form of A.

5.33. Solve the following system using the augmented matrix M:

$$\begin{aligned} x + 3y - 2z + t &= 3 \\ 2x + 6y - 5z - 3t &= 7 \end{aligned}$$

Reduce the augmented matrix M to echelon form and then to row canonical form:

$$M = \begin{bmatrix} 1 & 3 & -2 & 1 & 3 \\ 2 & 6 & -5 & -3 & 7 \end{bmatrix} \sim \begin{bmatrix} 1 & 3 & -2 & 1 & 3 \\ 0 & 0 & 1 & -5 & 1 \end{bmatrix} \sim \begin{bmatrix} 1 & 3 & 0 & -9 & 5 \\ 0 & 0 & 1 & -5 & 1 \end{bmatrix}$$

Write down the system corresponding to the row canonical form of M, that is,

$$\begin{aligned} x + 3y \qquad\quad - 9t &= 5 \\ z - 5t &= 1 \end{aligned}$$

The leading unknowns x and z in the echelon form of the system are called the *basic variables*, and the remaining unknowns y and t are called the *free variables*. Transfer the free variables to the other side to obtain the *free-variable* form of the solution:

$$x = 5 - 3y + 9t$$
$$z = 1 + 5t$$

The *parametric* form of the solution can be obtained by setting the free variables equal to *parameters*, say $y = a$ and $t = b$. This process yields

$$x = 5 - 3a + 9t, \qquad y = a, \qquad z = 1 + 5b, \qquad t = b \qquad \text{or} \qquad u = (5 - 3a + 9t,\ a,\ 1 + 5b,\ b)$$

(which is another form of the solution).

A particular solution of the system can now be obtained by assigning any values to the free variables (or parameters) and solving for the basic variables using the free variable (or parametric) form of the solution. For example, setting $y = 2$, $t = 3$, we obtain $x = 26$, $z = 16$. Thus

$$x = 26, \qquad y = 2, \qquad z = 16, \qquad t = 3 \qquad \text{or} \qquad u = (26, 2, 16, 3)$$

is a particular solution of the system.

5.34. Solve the following system using the augmented matrix M:

$$x + y - 2z + 4t = 5$$
$$2x + 2y - 3z + t = 4$$
$$3x + 3y - 4z - 2t = 3$$

Reduce the augmented matrix M to echelon form and then to row canonical form:

$$M = \begin{bmatrix} 1 & 1 & -2 & 4 & 5 \\ 2 & 2 & -3 & 1 & 4 \\ 3 & 3 & -4 & -2 & 3 \end{bmatrix} \sim \begin{bmatrix} 1 & 1 & -2 & 4 & 5 \\ 0 & 0 & 1 & -7 & -6 \\ \cancel{0} & \cancel{0} & \cancel{2} & \cancel{14} & \cancel{12} \end{bmatrix} \sim \begin{bmatrix} 1 & 1 & 0 & -10 & -7 \\ 0 & 0 & 1 & -7 & -6 \end{bmatrix}$$

(The third row of the second matrix is deleted since it is a multiple of the second row and will result in a zero row.)

Write down the system corresponding to the row canonical form of M and then transfer the free variables to the other side to obtain the free variable form of the solution:

$$x + y - 10t = -7 \quad z - 7t = -6 \qquad \text{and then} \qquad x = -7 - y + 10t \quad z = -6 + 7t$$

Here x and z are the basic variables and y and t are the free variables.

5.35. Solve the following system using the augmented matrix M:

$$x - 2y + 4z = 2$$
$$2x - 3y + 5z = 3$$
$$3x - 4y + 6z = 7$$

First row reduce the augmented matrix M to echelon form:

$$M = \begin{bmatrix} 1 & -2 & 4 & 2 \\ 2 & -3 & 5 & 3 \\ 3 & -4 & 6 & 7 \end{bmatrix} \sim \begin{bmatrix} 1 & -2 & 4 & 2 \\ 0 & 1 & -3 & -1 \\ 0 & 2 & -6 & 1 \end{bmatrix} \sim \begin{bmatrix} 1 & -2 & 4 & 2 \\ 0 & 1 & -3 & -1 \\ 0 & 0 & 0 & 3 \end{bmatrix}$$

In echelon form, the third row corresponds to the degenerate equation

$$0x + 0y + 0z = 3$$

Thus the system has no solution. (Note that the echelon form indicates whether or not the system has a solution.)

MISCELLANEOUS PROBLEMS

5.36. Let $A = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$ be Boolean matrices.

Find the Boolean products AB, BA, and A^2.

Find the usual matrix product and then substitute 1 for any nonzero scalar. Thus:

$$AB = \begin{bmatrix} 0 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}; \qquad BA = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}; \qquad A^2 = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$$

5.37. Let $A = \begin{bmatrix} 1 & 3 \\ 4 & -3 \end{bmatrix}$. (*a*) Find a nonzero column vector $u = \begin{bmatrix} x \\ y \end{bmatrix}$ such that $Au = 3u$. (*b*) Describe all such vectors.

(*a*) First set up the matrix equation $Au = 3u$ and then write each side as a single matrix (column vector):

$$\begin{bmatrix} 1 & 3 \\ 4 & -3 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = 3 \begin{bmatrix} x \\ y \end{bmatrix} \qquad \text{and} \qquad \begin{bmatrix} x + 3y \\ 4x - 3y \end{bmatrix} = \begin{bmatrix} 3x \\ 3y \end{bmatrix}$$

Set corresponding elements equal to each other to obtain a system of equations, and reduce the system to echelon form:

$$\begin{matrix} x + 3y = 3x \\ 4x - 3y = 3y \end{matrix} \quad \text{or} \quad \begin{matrix} 2x - 3y = 0 \\ 4x - 6y = 0 \end{matrix} \quad \text{to} \quad \begin{matrix} 2x - 3y = 0 \\ 0 = 0 \end{matrix} \quad \text{or} \quad 2x - 3y = 0$$

The system reduces to one (nondegenerate) linear equation in two unknowns, and so it has an infinite number of solutions. To obtain a nonzero solution, set $y = 2$, say; then $x = 3$. Thus $u = [3, 2]^T$ is a desired nonzero solution.

(*b*) To find the general solution, set $y = a$, where a is a parameter. Substitute $y = a$ into $2x - 3y = 0$ to obtain $x = 3a/2$. Thus $u = [3a/2, a]^T$ represents all such solutions.

Supplementary Problems

VECTORS

5.38. Let $u = (1, -2, 4)$, $v = (3, 5, 1)$, $w = (2, 1, -3)$. Find: (*a*) $3u - 2v$; (*b*) $4u - v - 3w$; (*c*) $5u + 7v - 2w$.

5.39. For the vectors in the preceding Problem 5.38, find:

(*a*) $u \cdot v$, $u \cdot w$, $v \cdot w$; (*b*) $\|u\|$, $\|v\|$, $\|w\|$.

5.40. Let $u = (2, -1, 0, -3)$, $v = (1, -1, -1, 3)$, $w = (1, 3, -2, 2)$. Find: (*a*) $2u - 3v$; (*b*) $5u - 3v - 4w$; (*c*) $-u + 2v - 2w$; (*d*) $u \cdot v$, $u \cdot w$, $v \cdot w$; (*e*) $\|u\|$, $\|v\|$, $\|w\|$.

5.41. Let $u = \begin{bmatrix} 1 \\ 3 \\ -4 \end{bmatrix}$, $v = \begin{bmatrix} 2 \\ 1 \\ 5 \end{bmatrix}$, $w = \begin{bmatrix} 3 \\ -2 \\ 6 \end{bmatrix}$. Find: (*a*) $5u - 3v$; (*b*) $2u + 4v - 6w$; (*c*) $u \cdot v$, $u \cdot w$, $v \cdot w$; (*d*) $\|u\|$, $\|v\|$, $\|w\|$.

5.42. Find x and y where: (*a*) $x(2,5) + y(4,-3) = (8,33)$; (*b*) $x(1,4) + y(2,-5) = (7,2)$.

5.43. Find x, y, z where $x\begin{bmatrix}1\\2\\3\end{bmatrix} + y\begin{bmatrix}2\\5\\-1\end{bmatrix} + z\begin{bmatrix}4\\-2\\3\end{bmatrix} = \begin{bmatrix}9\\-3\\16\end{bmatrix}$.

MATRIX OPERATIONS

Problem 5.44 through 5.48 refer to the following matrices:

$$A = \begin{bmatrix}1 & 2\\3 & -4\end{bmatrix}, \qquad B = \begin{bmatrix}5 & 0\\-6 & 7\end{bmatrix}; \qquad C = \begin{bmatrix}1 & -3 & 4\\2 & 6 & -5\end{bmatrix}; \qquad D = \begin{bmatrix}3 & 7 & -1\\4 & -8 & 9\end{bmatrix}$$

5.44. Find: (*a*) $5A - 2B$; (*b*) $c + D$; (*c*) $2c - 3D$.

5.45. Find: (*a*) AB; (*b*) BA.

5.46. Find: (*a*) AC; (*b*) AD; (*c*) BC; (*d*) BD.

5.47. Find: (*a*) A^T; (*b*) C^T; (*c*) C^TC; (*d*) CC^T.

5.48. Find: (*a*) $A^2 = AA$; (*b*) $B^2 = BB$; (*c*) $C^2 = CC$.

Problems 5.49 through 5.52 refer to the following matrices:

$$A = \begin{bmatrix}1 & -1 & 2\\0 & 3 & 4\end{bmatrix}; \qquad B = \begin{bmatrix}4 & 0 & -3\\-1 & -2 & 3\end{bmatrix}; \qquad C = \begin{bmatrix}2 & -3 & 0 & 1\\5 & -1 & -4 & 2\\-1 & 0 & 0 & 3\end{bmatrix}; \qquad D = \begin{bmatrix}2\\-1\\3\end{bmatrix}$$

5.49. Find: (*a*) $A + B$; (*b*) $A + C$; (*c*) $3A - 4B$.

5.50. Find: (*a*) AB; (*b*) AC; (*c*) AD.

5.51. Find: (*a*) BC; (*b*) BD; (*c*) CD.

5.52. Find: (*a*) A^T; (*b*) A^TB; (*c*) A^TC.

5.53. Let $A = \begin{bmatrix}1 & 2\\3 & 6\end{bmatrix}$. Find a 2×3 matrix B with distinct entries such that $AB = 0$.

SQUARE MATRICES

5.54. Find the diagonal of each matrix:

(*a*) $\begin{bmatrix}2 & -7 & 8\\3 & -6 & -5\\4 & 0 & -1\end{bmatrix}$; (*b*) $\begin{bmatrix}1 & 2 & -9\\3 & 1 & 8\\5 & -6 & -1\end{bmatrix}$; (*c*) $\begin{bmatrix}3 & 4 & -8\\2 & -7 & 0\end{bmatrix}$.

5.55. Let $A = \begin{bmatrix}2 & -5\\3 & 1\end{bmatrix}$. Find:

(*a*) A^2 and A^3; (*b*) $f(A)$, where $f(x) = x^3 - 2x^2 - 5$; (*c*) $g(A)$, where $g(x) = x^2 - 3x + 17$.

5.56. Let $B = \begin{bmatrix}4 & -2\\1 & -6\end{bmatrix}$. Find:

(*a*) B^2 and B^3; (*b*) $f(B)$, where $f(x) = x^2 + 2x - 22$; (*c*) $g(B)$, where $g(x) = x^2 - 3x - 6$.

5.57. Let $A = \begin{bmatrix}6 & -4\\3 & -2\end{bmatrix}$. Find a nonzero column vector $u = \begin{bmatrix}x\\y\end{bmatrix}$ such that $Au = 4u$.

DETERMINANTS AND INVERSES

5.58. Compute the determinant of each matrix:

$$(a)\ \begin{bmatrix}2 & 5\\ 4 & 1\end{bmatrix};\quad (b)\ \begin{bmatrix}6 & 1\\ 3 & -2\end{bmatrix};\quad (c)\ \begin{bmatrix}4 & -5\\ 0 & 2\end{bmatrix};\quad (d)\ \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix};\quad (e)\ \begin{bmatrix}-2 & 8\\ -5 & -2\end{bmatrix}.$$

5.59. Compute the determinant of each matrix:

$$(a)\ \begin{bmatrix}2 & 1 & 1\\ 0 & 5 & -2\\ 1 & -3 & 4\end{bmatrix};\quad (b)\ \begin{bmatrix}3 & -2 & -4\\ 2 & 5 & -1\\ 0 & 6 & 1\end{bmatrix};\quad (c)\ \begin{bmatrix}-2 & -1 & 4\\ 6 & -3 & -2\\ 4 & 1 & 2\end{bmatrix};\quad (d)\ \begin{bmatrix}7 & 6 & 5\\ 1 & 2 & 1\\ 3 & -2 & 1\end{bmatrix}.$$

5.60. Find the inverse of each matrix (if it exists):

$$A=\begin{bmatrix}7 & 4\\ 5 & 3\end{bmatrix};\qquad B=\begin{bmatrix}2 & 3\\ 4 & 5\end{bmatrix};\qquad C=\begin{bmatrix}4 & -6\\ -2 & 3\end{bmatrix};\quad =\begin{bmatrix}5 & -2\\ 6 & -3\end{bmatrix}$$

5.61. Find the inverse of each matrix (if it exists):

$$A=\begin{bmatrix}1 & 2 & -4\\ -1 & -1 & 5\\ 2 & 7 & -3\end{bmatrix}];\qquad B=\begin{bmatrix}1 & -1 & 1\\ 0 & 2 & -2\\ 1 & 3 & -1\end{bmatrix}]];\qquad C=\begin{bmatrix}1 & 2 & 3\\ 2 & 5 & -1\\ 5 & 12 & 1\end{bmatrix}]]$$

ECHELON MATRICES, ROW REDUCTION, GAUSSIAN ELIMINATION

5.62. Reduce A to echelon form and then to row canonical form, where:

$$(a)\quad A=\begin{bmatrix}1 & 2 & -1 & 2 & 1\\ 2 & 4 & 1 & -2 & 3\\ 3 & 6 & 2 & -6 & 5\end{bmatrix};\qquad (b)\quad A=\begin{bmatrix}2 & 3 & -2 & 5 & 1\\ 3 & -1 & 2 & 0 & 4\\ 4 & -5 & 6 & -5 & 7\end{bmatrix}.$$

5.63. Using only 0s and 1s, list all possible 2×2 matrices in echelon form.

5.64. Using only 0s and 1s, find the number of possible 3×3 matrices in row canonical form.

5.65. Solve each system using its augmented matrix M:

$$(a)\quad \begin{aligned} x+\ 2y-4z&=-3\\ 2x+\ 6y-5z&=\ 2\\ 3x+11y-4z&=\ 12\end{aligned}\qquad (b)\quad \begin{aligned} x+\ 2y-4z&=\ 3\\ 2x+\ 6y-5z&=10\\ 3x+10y-6z&=14\end{aligned}$$

5.66. Solve each system using its augmented matrix M:

$$(a)\quad \begin{aligned} x-3y+2z-\ t&=2\\ 3x-9y+7z-\ t&=7\\ 2x-6y+7z+4t&=7\end{aligned}\qquad (b)\quad \begin{aligned} x+\ 2y+3z&=\ 7\\ x+\ 3y+\ z&=\ 6\\ 2x+\ 6y+5z&=15\\ 3x+10y+7z&=23\end{aligned}$$

MISCELLANEOUS PROBLEMS

5.67. Let $A=\begin{bmatrix}1 & 2\\ 0 & 1\end{bmatrix}$. Find A^n.

5.68. Matrices A and B are said to commute if $AB=BA$. Find all matrices $\begin{bmatrix}x & y\\ z & t\end{bmatrix}$ which commute with $\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}$.

5.69. Let $A = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix}$ be Boolean matrices.

Find the Boolean matrices: (*a*) $A + B$; (*b*) AB; (*c*) BA; (*d*) A^2; (*e*) B^2.

Answers to Supplementary Problems

5.38. (*a*) $(-3, -16, 10)$; (*b*) $(-5, -16, 24)$; (*c*) $(22, 23, 33)$.

5.39. (*a*) $-3, -12, 8$; (*b*) $\sqrt{21}, \sqrt{35}, \sqrt{14}$.

5.40. (*a*) $(1, 1, 3, -15)$; (*b*) $(3, -14, 11, -32)$; (*c*) $(-2, -7, 2, 5)$; (*d*) $-6, -7, 6$; (*e*) $\sqrt{14}, \sqrt{12} = 2\sqrt{3}$, $\sqrt{18} = 3\sqrt{2}$.

5.41. (*a*) $(-1, 12, -35)^T$; (*b*) $(-8, 22, -24)^T$; (*c*) $-15, -27, 34$; (*d*) $\sqrt{26}, \sqrt{30}, 7$.

5.42. (*a*) $x = 2, y = -1$; (*b*) $x = 3, y = 2$.

5.43. $x = 3, y = -1, z = 2$.

5.44. (*a*) $\begin{bmatrix} -5 & 10 \\ 27 & -34 \end{bmatrix}$; (*b*) $\begin{bmatrix} 4 & 4 & 3 \\ 6 & -2 & 4 \end{bmatrix}$; (*c*) $= \begin{bmatrix} -7 & -27 & 11 \\ -8 & 36 & -37 \end{bmatrix}$.

5.45. $AB = \begin{bmatrix} -7 & 14 \\ 39 & -28 \end{bmatrix}$; $BA = \begin{bmatrix} 5 & 10 \\ 15 & -40 \end{bmatrix}$.

5.46. $AC = \begin{bmatrix} 5 & 9 & -6 \\ -5 & -33 & 32 \end{bmatrix}$; $AD = \begin{bmatrix} 11 & -9 & 17 \\ -7 & 53 & -39 \end{bmatrix}$; $BC = \begin{bmatrix} 5 & -15 & 20 \\ 8 & 60 & -59 \end{bmatrix}$; $BD = \begin{bmatrix} 15 & 35 & -5 \\ 10 & -98 & 69 \end{bmatrix}$.

5.47. $A^T = \begin{bmatrix} 1 & 3 \\ 2 & -4 \end{bmatrix}$; $C^T = \begin{bmatrix} 1 & 2 \\ -3 & 6 \\ 4 & -5 \end{bmatrix}$; $C^TC = \begin{bmatrix} 5 & 9 & -6 \\ 9 & 45 & -42 \\ -6 & -42 & 41 \end{bmatrix}$; $CC^T = \begin{bmatrix} 26 & -36 \\ -36 & 65 \end{bmatrix}$.

5.48. $A^2 = \begin{bmatrix} 7 & -6 \\ -9 & 22 \end{bmatrix}$; $B^2 = \begin{bmatrix} 25 & 0 \\ -72 & 49 \end{bmatrix}$; C^2 not defined.

5.49. (*a*) $\begin{bmatrix} 5 & -1 & -1 \\ -1 & 1 & 7 \end{bmatrix}$; (*b*) not defined; (*c*) $\begin{bmatrix} -13 & -3 & 18 \\ 4 & 17 & 0 \end{bmatrix}$.

5.50. AB not defined; $AC = \begin{bmatrix} -5 & -22 & 4 & 5 \\ 11 & -3 & -12 & 18 \end{bmatrix}$; $AD = \begin{bmatrix} 9 \\ 9 \end{bmatrix}$.

5.51. $BC = \begin{bmatrix} 11 & -12 & 0 & -5 \\ -15 & 5 & 8 & 4 \end{bmatrix}$; $BD = \begin{bmatrix} 11 \\ 9 \end{bmatrix}$; CD not defined.

5.52. $A^T = \begin{bmatrix} 1 & 0 \\ -1 & 3 \\ 2 & 4 \end{bmatrix}$; $A^TB = \begin{bmatrix} 4 & 0 & -3 \\ -7 & -6 & 12 \\ 4 & -8 & 6 \end{bmatrix}$; A^TC not defined.

5.53. $B = \begin{bmatrix} 2 & 4 \\ -1 & -2 \end{bmatrix}$.

5.54. (*a*) $[2, -6, -1$; (*b*) $[1, 1, -1]$; (*c*) not defined.

5.55. $A^2 = \begin{bmatrix} -11 & -15 \\ 9 & -14 \end{bmatrix}$; $A^3 = \begin{bmatrix} -67 & 40 \\ -24 & -59 \end{bmatrix}$; $f(A) = \begin{bmatrix} -50 & 70 \\ -42 & -36 \end{bmatrix}$; $g(A) = 0$.

5.56. $B^2 = \begin{bmatrix} 14 & 4 \\ -2 & 34 \end{bmatrix}$; $B^3 = \begin{bmatrix} 60 & -52 \\ 26 & -200 \end{bmatrix}$; $f(B) = 0$; $g(B) = \begin{bmatrix} -4 & 10 \\ -5 & 46 \end{bmatrix}$.

5.57. $u = (2a, a)^T$, for any nonzero a.

5.58. (*a*) -18; (*b*) -15; (*c*) 8; (*d*) 1; (*e*) 44.

5.59. (*a*) 21; (*b*) -11; (*c*) 100; (*d*) 0.

5.60. $A^{-1} = \begin{bmatrix} 3 & -4 \\ -5 & 7 \end{bmatrix}$; $B^{-1} = \begin{bmatrix} -\frac{5}{2} & \frac{3}{2} \\ 2 & -1 \end{bmatrix}$; C^{-1} not defined; $D^{-1} = \begin{bmatrix} 1 & -\frac{2}{3} \\ 2 & -\frac{5}{3} \end{bmatrix}$.

5.61. $A^{-1} = \begin{bmatrix} -16 & -11 & 3 \\ \frac{7}{2} & \frac{5}{2} & -\frac{1}{2} \\ -\frac{5}{2} & -\frac{3}{2} & \frac{1}{2} \end{bmatrix}$; $B^{-1} = \begin{bmatrix} 1 & \frac{1}{2} & 0 \\ -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \\ -\frac{1}{2} & -1 & \frac{1}{2} \end{bmatrix}$; C^{-1} not defined.

5.62. (*a*) $\begin{bmatrix} 1 & 2 & -1 & 2 & 1 \\ 0 & 0 & 3 & -6 & 1 \\ 0 & 0 & 0 & -6 & 1 \end{bmatrix}$ and $\begin{bmatrix} 1 & 2 & 0 & 0 & \frac{4}{3} \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & -\frac{1}{6} \end{bmatrix}$.

(*b*) $\begin{bmatrix} 2 & 3 & -2 & 5 & 1 \\ 0 & -11 & 10 & -15 & 5 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$ and $\begin{bmatrix} 1 & 0 & \frac{4}{11} & \frac{5}{11} & \frac{13}{11} \\ 0 & 1 & -\frac{10}{11} & \frac{15}{11} & -\frac{5}{11} \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$.

5.63. $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, $\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$, $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$, $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$, $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$.

5.64. There are 13.

5.65. (*a*) $x = 3$, $y = 1$, $z = 2$; (*b*) no solution.

5.66. (*a*) $x = 3y + 5t$, $y = 1 - 2t$; (*b*) $x = 2$, $y = 1$, $z = 1$.

5.67. $A^n = \begin{bmatrix} 1 & 2n \\ 0 & 1 \end{bmatrix}$.

5.68. $\begin{bmatrix} a & b \\ 0 & a \end{bmatrix}$.

5.69. $A + B = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}$; $AB = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix}$; $BA = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$; $A^2 = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix}$; $B^2 = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}$.

© The McGraw–Hill Companies, 2004

Chapter 6

Counting

6.1 INTRODUCTION, BASIC COUNTING PRINCIPLES

Combinatorial analysis, which includes the study of permutations, combinations, and partitions, is concerned with determining the number of logical possibilities of some event without necessarily identifying every case. There are two basic counting principles used throughout.

Sum Rule Principle: Suppose some event E can occur in m ways and a second event F can occur in n ways, and suppose both events cannot occur simultaneously. Then E or F can occur in $m + n$ ways. More generally, suppose an event E_1 can occur in n_1 ways, a second event E_2 can occur in n_2 ways, a third event E_3 can occur in n_3 ways, ..., and suppose no two of the events can occur at the same time. Then one of the events can occur in $n_1 + n_2 + n_3 + \cdots$ ways.

EXAMPLE 6.1

(*a*) Suppose there are 8 male professors and 5 female professors teaching a calculus class. A student can choose a calculus professor in $8 + 5 = 13$ ways.

(*b*) Suppose E is the event of choosing a prime number less than 10, and suppose F is the event of choosing an even number less than 10. Then E can occur in four ways $[2, 3, 5, 7]$, and F can occur in 4 ways $[2, 4, 6, 8]$. However E or F cannot occur in $4 + 4 = 8$ ways since 2 is both a prime number less than 10 and an even less than 10. In fact, E or F can occur in only $4 + 4 - 1 = 7$ ways.

(*c*) Suppose E is the event of choosing a prime number between 10 and 20, and suppose F is the event of choosing an even number between 10 and 20. Then E can occur in 4 ways $[11, 13, 17, 19]$, and F can occur in 4 ways $[12, 14, 16, 18]$. Then E or F can occur in $4 + 4 = 8$ ways since now none of the even numbers is prime.

Product Rule Principle: Suppose there is an event E which can occur in m ways and, independent of this event, there is a second event F which can occur in n ways. Then combinations of E and F can occur in mn ways. More generally, suppose an event E_1 can occur in n_1 ways, and, following E_1, a second event E_2 can occur in n_2 ways, and, following E_2, a third event E_3 can occur in n_3 ways, and so on. Then all the events can occur in the order indicated in $n_1 \cdot n_2 \cdot n_3 \cdots$ ways.

EXAMPLE 6.2

(*a*) Suppose a license plate contains two letters followed by three digits with the first digit not zero. How many different license plates can be printed?

Each letter can be printed in 26 different ways, the first digit in 9 ways and each of the other two digits in 10 ways. Hence

$$26 \cdot 26 \cdot 9 \cdot 10 \cdot 10 = 608\,400$$

different plates can be printed.

(*b*) In how many ways can an organization containing 26 members elect a president, treasurer, and secretary (assuming no person is elected to more than one position)?

The president can be elected in 26 different ways; following this, the treasurer can be elected in 25 different ways (since the person chosen president is not eligible to be treasurer); and, following this, the secretary can be elected in 24 different ways. Thus, by the above principle of counting, there are

$$26 \cdot 25 \cdot 24 = 15\,600$$

different ways in which the organization can elect the officers.

There is a set theoretical interpretation of the above two counting principles. Specifically, suppose $n(A)$ denotes the number of elements in a set A. Then:

(1) ***Sum Rule Principle:*** If A and B are disjoint sets, then

$$n(A \cup B) = n(A) + n(B)$$

(2) ***Product Rule Principle:*** Let $A \times B$ be the Cartesian product of sets A and B. Then

$$n(A \times B) = n(A) \cdot n(B)$$

6.2 FACTORIAL NOTATION

The product of the positive integers from 1 to n inclusive is denoted by $n!$ (read "n factorial"):

$$n! = 1 \cdot 2 \cdot 3 \cdot \cdots \cdot (n-2)(n-1)n$$

In other words, $n!$ is defined by

$$1! = 1 \qquad \text{and} \qquad n! = n \cdot (n-1)!$$

It is also convenient to define $0! = 1$.

EXAMPLE 6.3

(*a*) $2! = 1 \cdot 2 = 2, \quad 3! = 1 \cdot 2 \cdot 3 = 6, \quad 4! = 1 \cdot 2 \cdot 3 \cdot 4 = 24,$

$5! = 5 \cdot 4! = 5 \cdot 24 = 120, \quad 6! = 6 \cdot 5! = 6 \cdot 120 = 720.$

(*b*) $\dfrac{8!}{6!} = \dfrac{8 \cdot 7 \cdot 6!}{6!} = 8 \cdot 7 = 56, \quad 12 \cdot 11 \cdot 10 = \dfrac{12 \cdot 11 \cdot 10 \cdot 9!}{9!} = \dfrac{12!}{9!},$

$\dfrac{12 \cdot 11 \cdot 10}{1 \cdot 2 \cdot 3} = 12 \cdot 11 \cdot 10 \cdot \dfrac{1}{3!} = \dfrac{12!}{3!\,9!}.$

(*c*) $n(n-1)\cdots(n-r+1) = \dfrac{n(n-1)\cdots(n-r+1)(n-r)(n-r-1)\cdots 3 \cdot 2 \cdot 1}{(n-r)(n-r-1)\cdots 3 \cdot 2 \cdot 1} = \dfrac{n!}{(n-r)!}.$

$\dfrac{n(n-1)\cdots(n-r+1)}{1 \cdot 2 \cdot 3 \cdots (r-1)r} = n(n-1)\cdots(n-r+1) \cdot \dfrac{1}{r!} = \dfrac{n!}{(n-r)!} \cdot \dfrac{1}{r!} = \dfrac{n!}{r!(n-r)!}.$

6.3 BINOMIAL COEFFICIENTS

The symbol $\binom{n}{r}$ (*read* "*nCr*"), where r and n are positive integers with $r \le n$, is defined as follows

$$\binom{n}{r} = \frac{n(n-1)(n-2)\cdots(n-r+1)}{1 \cdot 2 \cdot 3 \cdots (r-1)r}$$

By Example 6.3(*c*), we see that

$$\binom{n}{r} = \frac{n(n-1)\cdots(n-r+1)}{1 \cdot 2 \cdot 3 \cdots (r-1)r} = \frac{n!}{r!(n-r)!}$$

But $n - (n-r) = r$; hence we have the following important relation:

$$\binom{n}{n-r} = \binom{n}{r} \text{ or, in other words, if } a + b = n \text{ then } \binom{n}{a} = \binom{n}{b}$$

EXAMPLE 6.4

(*a*) $\binom{8}{2} = \frac{8 \cdot 7}{1 \cdot 2} = 28, \quad \binom{9}{4} = \frac{9 \cdot 8 \cdot 7 \cdot 6}{1 \cdot 2 \cdot 3 \cdot 4} = 126, \quad \binom{12}{5} = \frac{12 \cdot 11 \cdot 10 \cdot 9 \cdot 8}{1 \cdot 2 \cdot 3 \cdot 4 \cdot 5} = 792,$

$\binom{10}{3} = \frac{10 \cdot 9 \cdot 8}{1 \cdot 2 \cdot 3} = 120, \quad \binom{13}{1} = \frac{13}{1} = 13.$

Note that $\binom{n}{r}$ has exactly r factors in both the numerator and the denominator.

(*b*) Compute $\binom{10}{7}$. By definition,

$$\binom{10}{7} = \frac{10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4}{1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7} = 120$$

On the other hand, $10 - 7 = 3$ and so we can also compute $\binom{10}{7}$ as follows:

$$\binom{10}{7} = \binom{10}{3} = \frac{10 \cdot 9 \cdot 8}{1 \cdot 2 \cdot 3} = 120$$

Observe that the second method saves space and time.

Binomial Coefficients and Pascal's Triangle

The numbers $\binom{n}{r}$ are called the *binomial coefficients* since they appear as the coefficients in the expansion of $(a+b)^n$. Specifically, one can prove that

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$$

The coefficients of the successive powers of $a+b$ can be arranged in a triangular array of numbers, called Pascal's triangle, as pictured in Fig. 6-1. The numbers in Pascal's triangle have the following intersecting properties:

(i) The first number and the last number in each row is 1.

(ii) Every other number in the array can be obtained by adding the two numbers appearing directly above it. For example $10 = 4 + 6$, $15 = 5 + 10$, $20 = 10 + 10$.

Since the numbers appearing in Pascal's triangle are binomial coefficients, property (ii) of Pascal's triangle comes from the following theorem (proved in Problem 6.7):

Theorem 6.1: $\binom{n+1}{r} = \binom{n}{r-1} + \binom{n}{r}$.

$$(a+b)^0 = 1$$
$$(a+b)^1 = a + b$$
$$(a+b)^2 = a^2 + 2ab + b^2$$
$$(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$$
$$(a+b)^4 = a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4$$
$$(a+b)^5 = a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 + b^5$$
$$(a+b)^6 = a^6 + 6a^5b + 15a^4b^2 + 20a^3b^3 + 15a^2b^4 + 6ab^5 + b^6$$
$$\cdots\cdots\cdots\cdots$$

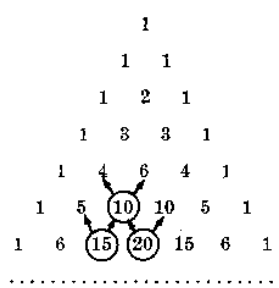


Fig. 6-1 Pascal's triangle.

6.4 PERMUTATIONS

Any arrangement of a set of n objects in a given order is called a *permutation* of the objects (taken all at a time). Any arrangement of any $r \leq n$ of these objects in a given order is called an *r-permutation* or a *permutation of the n objects taken r at a time*. Consider, for example, the set of letters a, b, c, and d. Then:

(i) *bdca*, *dcba* and *acdb* are permutations of the four letters (taken all at a time);
(ii) *bad*, *adb*, *cbd* and *bca* are permutations of the four letters taken three at a time;
(iii) *ad*, *cb*, *da* and *bd* are permutations of the four letters taken two at a time.

The number of permutations of n objects taken r at a time is denoted by

$$P(n,r),\ {}_nP_r, P_{n,r}, P_r^n, \text{ or } (n)_r$$

We shall use $P(n,r)$. Before we derive the general formula for $P(n,r)$ we consider a particular case.

EXAMPLE 6.5 Find the number of permutations of six objects, say A, B, C, D, E, F, taken three at a time. In other words, find the number of "three-letter words" using only the given six letters without repetitions.

Let the general three-letter word be represented by the following three boxes:

$$\&\quad \&\quad \&$$

Now the first letter can be chosen in six different ways; following this, the second letter can be chosen in five different ways; and, following this, the last letter can be chosen in four different ways. Write each number in its appropriate box as follows:

$$\boxed{6}\quad \boxed{5}\quad \boxed{4}$$

Thus by the fundamental principle of counting there are $6 \cdot 5 \cdot 4 = 120$ possible three-letter words without repetitions from the six letters, or there are 120 permutations of six objects taken three at a time:

$$P(6,3) = 120$$

Derivation of the Formula for *P(n, r)*

The derivation of the formula for the number of permutations of n objects taken r at a time, or the number of r-permutations of n objects, $P(n,r)$, follows the procedure in the preceding example. The first element in an r-permutation of n objects can be chosen in n different ways; following this, the second element in the permutation can be chosen in $n-1$ ways; and, following this, the third element in the permutation can be chosen in $n-2$ ways. Continuing in this manner, we have that the rth (last) element in the r-permutation can be chosen in $n-(r-1) = n-r+1$ ways. Thus, by the fundamental principle of counting, we have

$$P(n,r) = n(n-1)(n-2)\cdots(n-r+1)$$

By Example 6.3(c), we see that

$$n(n-1)(n-2)\cdots(n-r+1) = \frac{n(n-1)(n-2)\cdots(n-r+1)\cdot(n-r)!}{(n-r)!} = \frac{n!}{(n-r)!}$$

Thus we have proven the following theorem.

Theorem 6.2: $P(n,r) = \dfrac{n!}{(n-r)!}$.

In the special case in which $r = n$, we have

$$P(n,n) = n(n-1)(n-2)\cdots 3\cdot 2\cdot 1 = n!$$

Accordingly, we have the following corollary.

Corollary 6.3: There are $n!$ permutations of n objects (taken all at a time).

For example, there are $3! = 1 \cdot 2 \cdot 3 = 6$ permutations of the three letters a, b, and c. These are abc, acb, bac, bca, cab, cba.

Permutations with Repetitions

Frequently we want to know the number of permutations of a multiset, that is, a set of objects some of which are alike. We will let

$$P(n; n_1, n_2, \ldots, n_r)$$

denote the number of permutations of n objects of which n_1 are alike, n_2 are alike, ..., n_r are alike. The general formula follows:

Theorem 6.4: $P(n; n_1, n_2, \ldots, n_r) = \dfrac{n!}{n_1! n_2! \cdots n_r!}$.

We indicate the proof of the above theorem by a particular example. Suppose we want to form all possible five-letter "words" using the letters from the word "BABBY". Now there are $5! = 120$ permutations of the objects B_1, A, B_2, B_3, Y, where the three Bs are distinguished. Observe that the following six permutations

$$B_1B_2B_3AY, \quad B_2B_1B_3AY, \quad B_3B_1B_2AY, \quad B_1B_3B_2AY, \quad B_2B_3B_1AY, \quad B_3B_2B_1AY,$$

produce the same word when the subscripts are removed. The 6 comes from the fact that there are $3! = 3 \cdot 2 \cdot 1 = 6$ different ways of placing the three Bs in the first three positions in the permutation. This is true for each set of three positions in which the Bs can appear. Accordingly there are

$$P(5; 3) = \frac{5!}{3!} = \frac{120}{6} = 20$$

different five-letter words that can be formed using the letters from the word "BABBY".

EXAMPLE 6.6

(*a*) How many seven-letter words can be formed using the letters of the word "BENZENE"? We seek the number of permutations of seven objects of which three are alike (the three Es), and two are alike (the two Ns). By Theorem 6.4, the number of such words is

$$P(7; 3, 2) = \frac{7!}{3!\,2!} = \frac{7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1}{3 \cdot 2 \cdot 1 \cdot 2 \cdot 1} = 420$$

(*b*) How many different signals, each consisting of eight flags hung in a vertical line, can be formed from a set of four indistinguishable red flags, three indistinguishable white flags, and a blue flag? We seek the number of permutations of eight objects of which four are alike and three are alike. The number of such signals is

$$P(8; 4, 3) = \frac{8!}{4!\,3!} = \frac{8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1}{4 \cdot 3 \cdot 2 \cdot 1 \cdot 3 \cdot 2 \cdot 1} = 280$$

6.5 COMBINATIONS

Suppose we have a collection of n objects. A *combination* of these n objects taken r at a time is any selection of r of the objects where order does not count. In other words, an *r-combination* of a set of n objects is any subset of r elements. For example, the combinations of the letters a, b, c, d taken three at a time are

$$\{a, b, c\}, \quad \{a, b, d\}, \quad \{a, c, d\}, \quad \{b, c, d\} \qquad \text{or simply} \qquad abc,\ abd,\ acd,\ bcd$$

Observe that the following combinations are equal:

$$abc,\ acb,\ bac,\ bca,\ cab, \text{ and } cba$$

That is, each denotes the same set $\{a, b, c\}$.

The number of combinations of n objects taken r at a time is denoted by $C(n, r)$. The symbols ${}_nC_r$, $C_{n,r}$, and C_r^n also appear in various texts. Before we give the general formula for $C(n, r)$, we consider a special case.

EXAMPLE 6.7 Find the number of combinations of the four objects, a, b, c, d, taken three at a time.

Each combination consisting of three objects determines $3! = 6$ permutations of the objects in the combination as pictured in Fig. 6-2. Thus the number of combinations multiplied by 3! equals the number of permutations; that is,

$$C(4, 3) \cdot 3! = P(4, 3) \qquad \text{or} \qquad C(4, 3) = \frac{P(4, 3)}{3!}$$

But $P(4, 3) = 4 \cdot 3 \cdot 2 = 24$ and $3! = 6$; hence $C(4, 3) = 4$ as noted in Fig. 6-2.

Combination	Permutations
abc	*abc, acb, bac, bca, cab, cba*
abd	*abd, adb, bad, bda, dab, dba*
acd	*acd, adc, cad, cda, dac, dca*
bcd	*bcd, bdc, cbd, cdb, dbc, dcb*

Fig. 6-2

Formula for $C(n, r)$

Since any combination of n objects taken r at a time determines $r!$ permutations of the objects in the combination, we can conclude that

$$P(n, r) = r!C(n, r)$$

Thus we obtain

Theorem 6.5: $C(n, r) = \dfrac{P(n, r)}{r!} = \dfrac{n!}{r!(n - r)!}$

Recall that the binomial coefficient $\binom{n}{r}$ was defined to be $\dfrac{n!}{r!(n - r)!}$; hence

$$C(n, r) = \binom{n}{r}$$

We shall use $C(n, r)$ and $\binom{n}{r}$ interchangeably.

EXAMPLE 6.8

(*a*) How many committees of three can be formed from eight people?

Each committee is, essentially, a combination of the eight people taken three at a time. Thus the number of committees that can be formed is

$$C(8, 3) = \binom{8}{3} = \frac{8 \cdot 7 \cdot 6}{1 \cdot 2 \cdot 3} = 56$$

(*b*) A farmer buys 3 cows, 2 pigs and 4 hens from a man who has 6 cows, 5 pigs and 8 hens. How many choices does the farmer have?

The farmer can choose the cows in $\binom{6}{3}$ ways, the pigs in $\binom{5}{2}$ ways, and the hens in $\binom{8}{4}$ ways.

Hence altogether he can choose the animals in

$$\binom{6}{3}\binom{5}{2}\binom{8}{4} = \frac{6\cdot 5\cdot 4}{1\cdot 2\cdot 3}\cdot\frac{5\cdot 4}{1\cdot 2}\cdot\frac{8\cdot 7\cdot 6\cdot 5}{1\cdot 2\cdot 3\cdot 4} = 20\cdot 10\cdot 70 = 14\,000 \text{ ways}$$

6.6 THE PIGEONHOLE PRINCIPLE

Many results in combinatorial theory come from the following almost obvious statement.

Pigeonhole Principle: If n pigeonholes are occupied by $n+1$ or more pigeons, then at least one pigeonhole is occupied by more than one pigeon.

This principle can be applied to many problems where we want to show that a given situation can occur.

EXAMPLE 6.9

(*a*) Suppose a department contains 13 professors. Then two of the professors (pigeons) were born in the same month (pigeonholes).

(*b*) Suppose a laundry bag contains many red, white, and blue socks. Then one need only grab four socks (pigeons) to be sure of getting a pair with the same color (pigeonholes).

(*c*) Find the minimum number of elements that one needs to take from the set $S = \{1, 2, 3, \ldots, 9\}$ to be sure that two of the numbers add up to 10.

Here the pigeonholes are the five sets $\{1, 9\}$, $\{2, 8\}$, $\{3, 7\}$, $\{4, 6\}$, $\{5\}$. Thus any choice of six elements (pigeons) of S will guarantee that two of the numbers add up to ten.

The Pigeonhole Principle is generalized as follows.

Generalized Pigeonhole Principle: If n pigeonholes are occupied by $kn+1$ or more pigeons, where k is a positive integer, then at least one pigeonhole is occupied by $k+1$ or more pigeons.

EXAMPLE 6.10

(*a*) Find the minimum number of students in a class to be sure that three of them are born in the same month.

Here the $n = 12$ months are the pigeonholes and $k+1 = 3$, or $k = 2$. Hence among any $kn+1 = 25$ students (pigeons), three of them are born in the same month.

(*b*) Suppose a laundrybag contains many red, white, and blue socks. Find the minimum number of socks that one needs to choose in order to get two pairs (four socks) of the same color.

Here there are $n = 3$ colors (pigeonholes) and $k+1 = 4$, or $k = 3$. Thus among any $kn+1 = 10$ socks (pigeons), four of them have the same color.

6.7 THE INCLUSION–EXCLUSION PRINCIPLE

Let A and B be any finite sets. Then

$$n(A \cup B) = n(A) + n(B) - n(A \cap B)$$

In other words, to find the number $n(A \cup B)$ of elements in the union $A \cup B$, we add $n(A)$ and $n(B)$ and then we subtract $n(A \cap B)$; that is, we "include" $n(A)$ and $n(B)$, and we "exclude" $n(A \cap B)$. This follows from the fact that, when we add $n(A)$ and $n(B)$, we have counted the elements of $A \cap B$ twice. This principle holds for any number of sets. We first state it for three sets.

Theorem 6.6: For any finite sets A, B, C we have

$$n(A \cup B \cup C) = n(A) + n(B) + n(C) - n(A \cap B) - n(A \cap C) - n(B \cap C) + n(A \cap B \cap C)$$

That is, we "include" $n(A)$, $n(B)$, $n(C)$, we "exclude" $n(A \cap B)$, $n(A \cap C)$, $n(B \cap C)$, and we include $n(A \cap B \cap C)$.

EXAMPLE 6.11 Find the number of mathematics students at a college taking at least one of the languages French, German, and Russian given the following data:

65 study French	20 study French and German
45 study German	25 study French and Russian
42 study Russian	15 study German and Russian
	8 study all three languages

We want to find $n(F \cup G \cup R)$ where F, G, and R denote the sets of students studying French, German, and Russian, respectively.

By the inclusion–exclusion principle,

$$n(F \cup G \cup R) = n(F) + n(G) + n(R) - n(F \cap G) - n(F \cap R) - n(G \cap R) + n(F \cap G \cap R)$$

$$= 65 + 45 + 42 - 20 - 25 - 15 + 8 = 100$$

Thus 100 students study at least one of the languages.

Now, suppose we have any finite number of finite sets, say, $A_1, A_2, \ldots, A_m$. Let s_k be the sum of the cardinalities

$$n(A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_k})$$

of all possible k-tuple intersections of the given m sets. Then we have the following general inclusion–exclusion principle.

Theorem 6.7: $n(A_1 \cup A_2 \cup \cdots \cup A_m) = s_1 - s_2 + s_3 - \cdots + (-1)^{m-1} s_m$.

6.8 ORDERED AND UNORDERED PARTITIONS

Suppose a bag A contains seven marbles numbered 1 through 7. We compute the number of ways we can draw, first, two marbles from the bag, then three marbles from the bag, and lastly two marbles from the bag. In other words, we want to compute the number of *ordered partitions*

$$[A_1, A_2, A_3]$$

of the set of seven marbles into cells A_1 containing two marbles, A_2 containing three marbles and A_3 containing two marbles. We call these ordered partitions since we distinguish between

$$[\{1,2\}, \{3,4,5\}, \{6,7\}] \quad \text{and} \quad [\{6,7\}, \{3,4,5\}, \{1,2\}]$$

each of which determines the same partition of A.

Now we begin with seven marbles in the bag, so there are $\binom{7}{2}$ ways of drawing the first two marbles, i.e., of determining the first cell A_1; following this, there are five marbles left in the bag and so there are $\binom{5}{3}$ ways of drawing the three marbles, i.e., of determining the second cell A_2; finally, there are two marbles left in the bag and so there are $\binom{2}{2}$ ways of determining the last cell A_3. Hence there are

$$\binom{7}{2}\binom{5}{3}\binom{2}{2} = \frac{7 \cdot 6}{1 \cdot 2} \cdot \frac{5 \cdot 4 \cdot 3}{1 \cdot 2 \cdot 3} \cdot \frac{2 \cdot 1}{1 \cdot 2} = 210$$

different ordered partitions of A into cells A_1 containing two marbles, A_2 containing three marbles, and A_3 containing two marbles.

Now observe that

$$\binom{7}{2}\binom{5}{3}\binom{2}{2} = \frac{7!}{2!\,5!} \cdot \frac{5!}{3!\,2!} \cdot \frac{2!}{2!\,0!} = \frac{7!}{2!\,3!\,2!}$$

since each numerator after the first is canceled by the second term in the denominator of the previous factor.

The above discussion can be shown to hold in general. Namely,

Theorem 6.8: Let A contain n elements and let $n_1, n_2, \ldots, n_r$ be positive integers whose sum is n, that is, $n_1 + n_2 + \cdots + n_r = n$. Then there exist

$$\frac{n!}{n_1!\,n_2!\,n_3! \cdots n_r!}$$

different ordered partitions of A of the form $[A_1, A_2, \ldots, A_r]$ where A_1 contains n_1 elements, A_2 contains n_2 elements, ..., and A_r contains n_r elements.

We apply this theorem in the next example.

EXAMPLE 6.12 Find the number m of ways that nine toys can be divided between four children if the youngest child is to receive three toys and each of the others two toys.

We wish to find the number m of ordered partitions of the nine toys into four cells containing 3, 2, 2, 2 toys respectively. By Theorem 6.8,

$$m = \frac{9!}{3!\,2!\,2!\,2!} = 7560$$

Unordered Partitions

Frequently, we want to partition a set A into a collection of subsets $A_1, A_2, \ldots, A_r$ where the subsets are now unordered. Just as the number of permutations with repetitions was obtained from the number of permutations by dividing by $k!$ when k objects were alike, so too we can obtain the number of unordered partitions from the number of ordered partitions by dividing by $k!$ when k of the sets have the same number of elements. This is illustrated in the next example, where we solve the problem in two ways.

EXAMPLE 6.13 Find the number m of ways that 12 students can be partitioned into three teams, A_1, A_2, and A_3, so that each team contains four students.

Method 1: Let A denote one of the students. Then there are $\binom{11}{3}$ ways to choose three other students to be on the same team as A. Now let B denote a student who is not on the same team as A; then there are $\binom{7}{3}$ ways to choose three students of the remaining students to be on the same team as B. The remaining four students constitute the third team. Thus, altogether, the number of ways to partition the students is

$$m = \binom{11}{3} \cdot \binom{7}{3} = 165 \cdot 35 = 5775$$

Method 2: Observe that each partition $\{A_1, A_2, A_3\}$ of the students can be arranged in $3! = 6$ ways as an ordered partition. By Theorem 6.8, there are $\dfrac{12!}{4!\,4!\,4!} = 34\,650$ such ordered partitions. Thus there are $m = 34\,650/6 = 5775$ (unordered) partitions.

Solved Problems

FACTORIAL NOTATION AND BINOMIAL COEFFICIENTS

6.1. Compute $4!, 5!, 6!$, and $7!$.

$4! = 1 \cdot 2 \cdot 3 \cdot 4 = 24$, $\quad 6! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 = 6 \cdot (5!) = 6 \cdot (120) = 720$,

$5! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 = 5 \cdot (4!) = 5 \cdot (24) = 120$, $\quad 7! = 7 \cdot (6!) = 7 \cdot (720) = 5040$.

6.2. Compute: (*a*) $\dfrac{13!}{11!}$; (*b*) $\dfrac{7!}{10!}$.

(*a*) $\dfrac{13!}{11!} = \dfrac{13 \cdot 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1}{11 \cdot 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1} = 13 \cdot 12 = 156.$

Alternatively, this could be solved as follows:

$$\frac{13!}{11!} = \frac{13 \cdot 12 \cdot 11!}{11!} = 13 \cdot 12 = 156.$$

(*b*) $\dfrac{7!}{10!} = \dfrac{7!}{10 \cdot 9 \cdot 8 \cdot 7!} = \dfrac{1}{10 \cdot 9 \cdot 8} = \dfrac{1}{720}.$

6.3. Simplify: (*a*) $\dfrac{n!}{(n-1)!}$; (*b*) $\dfrac{(n+2)!}{n!}$.

(*a*) $\dfrac{n!}{(n-1)!} = \dfrac{n(n-1)(n-2)\cdots 3 \cdot 2 \cdot 1}{(n-1)(n-2)\cdots 3 \cdot 2 \cdot 1} = n$; alternatively, $\dfrac{n!}{(n-1)!} = \dfrac{n(n-1)!}{(n-1)!} = n.$

(*b*) $\dfrac{(n+2)!}{n!} = \dfrac{(n+2)(n+1)n(n-1)(n-2)\cdots 3 \cdot 2 \cdot 1}{(n-1)(n-2)\cdots 3 \cdot 2 \cdot 1} = (n+2)(n+1) = n^2 + 3n + 2;$

alternatively, $\dfrac{(n+2)!}{n!} = \dfrac{(n+2)(n+1)n!}{n!} = (n+2)(n+1) = n^2 + 3n + 2.$

6.4. Compute: (*a*) $\binom{16}{3}$; (*b*) $\binom{12}{4}$.

Recall that there are as many factors in the numerator as in the denominator.

(*a*) $\binom{16}{3} = \dfrac{16 \cdot 15 \cdot 14}{1 \cdot 2 \cdot 3} = 560;$ (*b*) $\binom{12}{4} = \dfrac{12 \cdot 11 \cdot 10 \cdot 9}{1 \cdot 2 \cdot 3 \cdot 4} = 495.$

6.5. Compute: (*a*) $\binom{8}{5}$; (*b*) $\binom{9}{7}$.

(*a*) $\binom{8}{5} = \dfrac{8 \cdot 7 \cdot 6 \cdot 5 \cdot 4}{1 \cdot 2 \cdot 3 \cdot 4 \cdot 5} = 56$ or, since $8 - 5 = 3$, $\binom{8}{5} = \binom{8}{3} = \dfrac{8 \cdot 7 \cdot 6}{1 \cdot 2 \cdot 3} = 56.$

(*b*) Since $9 - 7 = 2$, we have $\binom{9}{7} = \binom{9}{2} = \frac{9 \cdot 8}{1 \cdot 2} = 36$.

6.6. Prove: $\binom{17}{6} = \binom{16}{5} + \binom{16}{6}$.

Now $\binom{16}{5} + \binom{16}{6} = \frac{16!}{5!\,11!} + \frac{16!}{6!\,10!}$. Multiply the first fraction by $\frac{6}{6}$ and the second by $\frac{11}{11}$ to obtain the same denominator in both fractions; and then add:

$$\binom{16}{5} + \binom{16}{6} = \frac{6 \cdot 16!}{6 \cdot 5! \cdot 11!} + \frac{11 \cdot 16!}{6! \cdot 11 \cdot 10!} = \frac{6 \cdot 16!}{6! \cdot 11!} + \frac{11 \cdot 16!}{6! \cdot 11!}$$
$$= \frac{6 \cdot 16! + 11 \cdot 16!}{6! \cdot 11!} = \frac{(6 + 11) \cdot 16!}{6! \cdot 11!} = \frac{17 \cdot 16!}{6! \cdot 11!} = \frac{17!}{6! \cdot 11!} = \binom{17}{6}$$

6.7. Prove Theorem 6.1: $\binom{n+1}{r} = \binom{n}{r-1} + \binom{n}{r}$.

(The technique in this proof is similar to that of the preceding problem.)

Now $\binom{n}{r-1} + \binom{n}{r} = \frac{n!}{(r-1)! \cdot (n-r+1)!} + \frac{n!}{r! \cdot (n-r)!}$. To obtain the same denominator in both fractions, multiply the first fraction by $\frac{r}{r}$ and the second fraction by $\frac{n-r+1}{n-r+1}$. Hence

$$\binom{n}{r-1} + \binom{n}{r} = \frac{r \cdot n!}{r \cdot (r-1)! \cdot (n-r+1)!} + \frac{(n-r+1) \cdot n!}{r! \cdot (n-r+1) \cdot (n-r)!}$$
$$= \frac{r \cdot n!}{r!(n-r+1)!} + \frac{(n-r+1) \cdot n!}{r!(n-r+1)!}$$
$$= \frac{r \cdot n! + (n-r+1) \cdot n!}{r!(n-r+1)!} = \frac{[r + (n-r+1)] \cdot n!}{r!(n-r+1)!}$$
$$= \frac{(n+1)n!}{r!(n-r+1)!} = \frac{(n+1)!}{r!(n-r+1)!} = \binom{n+1}{r}$$

PERMUTATIONS

6.8. There are four bus lines between A and B; and three bus lines between B and C. In how many ways can a man travel (*a*) by bus from A to C by way of B? (*b*) round-trip by bus from A to C by way of B? (*c*) round-trip by bus from A to C by way of B, if he does not want to use a bus line more than once?

(*a*) There are four ways to go from A to B and three ways to go from B to C; hence there are $4 \cdot 3 = 12$ ways to go from A to C by way of B.

(*b*) There are 12 ways to go from A to C by way of B, and 12 ways to return. Hence there are $12 \cdot 12 = 144$ ways to travel round-trip.

(*c*) The man will travel from A to B to C to B to A. Enter these letters with connecting arrows as follows:

$$A \longrightarrow B \longrightarrow C \longrightarrow B \longrightarrow A$$

The man can travel four ways from A to B and three ways from B to C, but he can only travel two ways from C to B and three ways from B to A since he does not want to use a bus line more than once. Enter these numbers above the corresponding arrows as follows:

$$A \xrightarrow{4} B \xrightarrow{3} C \xrightarrow{2} B \xrightarrow{3} A$$

Thus there are $4 \cdot 3 \cdot 2 \cdot 3 = 72$ ways to travel round-trip without using the same bus line more than once.

6.9. Suppose repetitions are not permitted. (*a*) How many three-digit numbers can be formed from the six digits 2, 3, 5, 6, 7, and 9? (*b*) How many of these numbers are less than 400? (*c*) How many are even?

In each case draw three boxes & & & to represent an arbitrary number, and then write in each box the number of digits that can be placed there.

(*a*) The box on the left can be filled in six ways; following this, the middle box can be filled in five ways; and, lastly, the box on the right can be filled in four ways: 6 5 4. Thus there are $6 \cdot 5 \cdot 4 = 120$ numbers.

(*b*) The box on the left can be filled in only two ways, by 2 or 3, since each number must be less than 400; the middle box can be filled in five ways; and, lastly, the box on the right can be filled in four ways: 2 5 4. Thus, there are $2 \cdot 5 \cdot 4 = 40$ numbers.

(*c*) The box on the right can be filled in only two ways, by 2 or 6, since the numbers must be even; the box on the left can then be filled in five ways; and, lastly, the middle box can be filled in four ways: 5 4 2. Thus, there are $5 \cdot 4 \cdot 2 = 40$ numbers.

6.10. Find the number of ways that a party of seven persons can arrange themselves: (*a*) in a row of seven chairs; (*b*) around a circular table.

(*a*) The seven persons can arrange themselves in a row in $7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 7!$ ways.

(*b*) One person can sit at any place in the circular table. The other six persons can then arrange themselves in $6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 6!$ ways around the table.

This is an example of a *circular permutation*. In general, n objects can be arranged in a circle in $(n-1)(n-2)\cdots 3 \cdot 2 \cdot 1 = (n-1)!$ ways.

6.11. Find the number of distinct permutations that can be formed from all the letters of each word: (*a*) RADAR; (*b*) UNUSUAL.

(*a*) $\dfrac{5!}{2!\,2!} = 30$, since there are five letters of which two are R and two are A.

(*b*) $\dfrac{7!}{3!} = 840$, since there are seven letters of which three are U.

6.12. In how many ways can four mathematics books, three history books, three chemistry books, and two sociology books be arranged on a shelf so that all books of the same subject are together?

First the books must be arranged on the shelf in four units according to subject matter: & & & &. The box on the left can be filled by any of the four subjects; the next by any three remaining subjects, the next by any two remaining subjects, and the box on the right by the last subject: 4 3 2 1. Thus there are $4 \cdot 3 \cdot 2 \cdot 1 = 4!$ ways to arrange the books on the shelf according to subject matter.

Now, in each of the above cases, the mathematics books can be arranged in 4! ways, the history books in 3! ways, the chemistry books in 3! ways, and the sociology books in 2! ways. Thus, altogether, there are $4! \cdot 4! \cdot 3! \cdot 3! \cdot 2! = 41\,472$ arrangements.

6.13. Find n if: (*a*) $P(n, 2) = 72$; (*b*) $P(n, 4) = 42P(n, 2)$; (*c*) $2P(n, 2) + 50 = P(2n, 2)$.

(*a*) $P(n, 2) = n(n-1) = n^2 - n$; hence $n^2 - n = 72$ or $n^2 - n - 72 = 0$ or $(n-9)(n+8) = 0$. Since n must be positive, the only answer is $n = 9$.

(*b*) $P(n, 4) = n(n-1)(n-2)(n-3)$ and $P(n, 2) = n(n-1)$. Hence

$$n(n-1)(n-2)(n-3) = 42n(n-1) \quad \text{or, if } n \neq 0, n \neq 1, \qquad (n-2)(n-3) = 42$$

$$\text{or} \qquad n^2 - 5n + 6 = 42 \qquad \text{or} \qquad n^2 - 5n - 36 = 0 \qquad \text{or} \qquad (n-9)(n+4) = 0$$

Since n must be positive, the only answer is $n = 9$.

(*c*) $P(n, 2) = n(n-1) = n^2 - n$ and $P(2n, 2) = 2n(2n-1) = 4n^2 - 2n$. Hence

$$2(n^2 - n) + 50 = 4n^2 - 2n \qquad \text{or} \qquad 2n^2 - 2n + 50 = 4n^2 - 2n \quad \text{or} \quad 50 = 2n^2 \quad \text{or} \quad n^2 = 25$$

Since n must be positive, the only answer is $n = 5$.

COMBINATIONS

6.14. In how many ways can a committee consisting of three men and two women be chosen from seven men and five women?

The three men can be chosen from the seven men in $\binom{7}{3}$ ways, and the two women can be chosen from the five women in $\binom{5}{2}$ ways. Hence the committee can be chosen in

$$\binom{7}{3}\binom{5}{2} = \frac{7 \cdot 6 \cdot 5}{1 \cdot 2 \cdot 3} \cdot \frac{5 \cdot 4}{1 \cdot 2} = 350 \text{ ways}$$

6.15. A bag contains six white marbles and five red marbles. Find the number of ways four marbles can be drawn from the bag if (*a*) they can be any color; (*b*) two must be white and two red; (*c*) they must all be of the same color.

(*a*) The four marbles (of any color) can be chosen from the eleven marbles in $\binom{11}{4} = \frac{11 \cdot 10 \cdot 9 \cdot 8}{1 \cdot 2 \cdot 3 \cdot 4} = 330$ ways.

(*b*) The two white marbles can be chosen in $\binom{6}{2}$ ways, and the two red marbles can be chosen in $\binom{5}{2}$ ways. Thus there are $\binom{6}{2}\binom{5}{2} = \frac{6 \cdot 5}{1 \cdot 2} \cdot \frac{5 \cdot 4}{1 \cdot 2} = 150$ ways of drawing two white marbles and two red marbles.

(*c*) There are $\binom{6}{4} = 15$ ways of drawing four white marbles, and $\binom{5}{4} = 5$ ways of drawing four red marbles. Thus there are $15 + 5 = 20$ ways of drawing four marbles of the same color.

6.16. How many committees of five with a given chairperson can be selected from 12 persons?

The chairperson can be chosen in 12 ways and, following this, the other four on the committee can be chosen from the eleven remaining in $\binom{11}{4}$ ways. Thus there are $12 \cdot \binom{11}{4} = 12 \cdot 330 = 3960$ such committees.

ORDERED AND UNORDERED PARTITIONS

6.17. In how many ways can nine students be partitioned into three teams containing four, three, and two students, respectively?

Since all the cells contain different numbers of students, the number of unordered partitions equals the number of ordered partitions, $\frac{9!}{4!\,3!\,2!} = 1260$

6.18. There are 12 students in a class. In how many ways can the 12 students take four different tests if three students are to take each test?

Method 1: We seek the number of ordered partitions of the 12 students into cells containing three students each. By Theorem 6.8, there are $\frac{12!}{3!\,3!\,3!\,3!} = 369\,600$ such partitions.

Method 2: There are $\binom{12}{3}$ ways to choose three students to take the first test; following this, there are $\binom{9}{3}$ ways to choose three students to take the second test, and $\binom{6}{3}$ ways to choose three students to take the third test. The remaining students take the fourth test. Thus, altogether, there are $\binom{12}{3}\binom{9}{3}\binom{6}{3} = (220)(84)(20) = 369\,600$ ways for the students to take the tests.

6.19. In how many ways can 12 students be partitioned into four teams, A_1, A_2, A_3, and A_4, so that each team contains three students?

Method 1: Observe that each partition $\{A_1, A_2, A_3, A_4\}$ of the students can be arranged in $4! = 24$ ways as an ordered partition. Since (see the preceding problem) there are $\frac{12!}{3!\,3!\,3!\,3!} = 369\,600$ such ordered partitions, there are $369\,600/24 = 15\,400$ (unordered) partitions.

Method 2: Let A denote one of the students. Then there are $\binom{11}{2}$ ways to choose two other students to be on the same team as A. Now let B denote a student who is not on the same team as A. Then there are $\binom{8}{2}$ ways to choose two students from the remaining students to be on the same team as B. Next let C denote a student who is not on the same team as A or B. Then there are $\binom{5}{2}$ ways to choose two students to be on the same team as C. The remaining three students constitute the fourth team. Thus, altogether, there are $\binom{11}{2}\binom{8}{2}\binom{5}{2} = (55)(28)(10) = 15\,400$ ways to partition the students.

THE PIGEONHOLE PRINCIPLE

6.20. Assume there are n distinct pairs of shoes in a closet. Show that if you choose $n + 1$ single shoes at random from the closet, you are certain to have a pair.

The n distinct pairs constitute n pigeonholes. The $n + 1$ single shoes correspond to $n + 1$ pigeons. Therefore, there must be at least one pigeonhole with two shoes and thus you will certainly have drawn at least one pair of shoes.

6.21. Assume there are three men and five women at a party. Show that if these people are lined up in a row, at least two women will be next to each other.

Consider the case where the men are placed so that no two men are next to each other and not at either end of the line. In this case, the three men generate four potential locations (pigeonholes) in which to place women (at either end of the line and two locations between men within the line). Since there are five women (pigeons), at least one slot will contain two women who must, therefore, be next to each other. If the men are allowed to be placed next to each other or at the end of the line, there are even fewer pigeonholes and, once again, at least two women will have to be placed next to each other.

6.22. Find the minimum number of students needed to guarantee that five of them belong to the same class (Freshman, Sophomore, Junior, Senior).

Here the $n = 4$ classes are the pigeonholes and $k + 1 = 5$ so $k = 4$. Thus among any $kn + 1 = 17$ students (pigeons), five of them belong to the same class.

6.23. A student must take five classes from three areas of study. Numerous classes are offered in each discipline, but the student cannot take more than two classes in any given area.

(*a*) Using the pigeonhole principle, show that the student will take at least two classes in one area.

(*b*) Using the inclusion–exclusion principle, show that the student will have to take at least one class in each area.

(*a*) The three areas are the pigeonholes and the student must take five classes (pigeons). Hence, the student must take at least two classes in one area.

(*b*) Let each of the three areas of study represent three disjoint sets, A, B, and C. Since the sets are disjoint, $m(A \cup B \cup C) = 5 = n(A) + n(B) + n(C)$. Since the student can take at most two classes in any area of study, the sum of classes in any two sets, say A and B, must be less than or equal to four. Hence, $5 - [n(A) + n(B)] = n(C) \geq 1$. Thus, the student must take at least one class in any area.

6.24. Let L be a list (not necessarily in alphabetical order) of the 26 letters in the English alphabet (which consists of 5 vowels, A, E, I, O, U, and 21 consonants). (*a*) Show that L has a sublist consisting of four or more consecutive consonants. (*b*) Assumming L begins with a vowel, say A, show that L has a sublist consisting of five or more consecutive consonants.

(*a*) The five letters partition L into $n = 6$ sublists (pigeonholes) of consecutive consonants. Here $k + 1 = 4$ and so $k = 3$. Hence $nk + 1 = 6(3) + 1 = 19 < 21$. Hence some sublist has at least four consecutive consonants.

(*b*) Since L begins with a vowel, the remainder of the vowels partition L into $n = 5$ sublists. Here $k + 1 = 5$ and so $k = 4$. Hence $kn + 1 = 21$. Thus some sublist has at least five consecutive consonants.

6.25. Find the minimum number n of integers to be selected from $S = \{1, 2, \ldots, 9\}$ so that: (*a*) the sum of two of the n integers is even; (*b*) the difference of two of the n integers is 5.

(*a*) The sum of two even integers or of two odd integers is even. Consider the subsets {1,3,5,7,9} and {2,4,6,8} of S as pigeonholes. Hence $n = 3$.

(*b*) Consider the five subsets {1,6}, {2,7}, {3,8}, {4,9}, {5} of S as pigeonholes. Then $n = 6$ will guarantee that two integers will belong to one of the subsets and their difference will be 5.

THE INCLUSION–EXCLUSION PRINCIPLE

6.26. There are 22 female students and 18 male students in a classroom. How many students are there in total?

The sets of male and female students are disjoint; hence the total $t = 22 + 18 = 40$ students.

6.27. Of 32 people who save paper or bottles (or both) for recycling, 30 save paper and 14 save bottles. Find the number m of people who (*a*) save both, (*b*) save only paper, and (*c*) save only bottles.

Let P and B denote the sets of people saving paper and bottles, respectively. By Theorem 6.7:

(*a*) $m = n(P \cap B) = n(P) + n(B) - n(P \cup B) = 30 + 14 - 32 = 12.$

(*b*) $m = n(P \setminus B) = n(P) - n(P \cap B) = 30 - 12 = 18.$

(*c*) $m = n(B \setminus P) = n(B) - n(P \cap B) = 14 - 12 = 2.$

6.28. Let A, B, C, D denote, respectively, art, biology, chemistry, and drama courses. Find the number N of students in a dormitory given the data:

12 take A,	5 take A and B,	3 take A, B, C,
20 take B,	7 take A and C,	2 take A, B, D,
20 take C,	4 take A and D,	2 take B, C, D,
8 take D,	16 take B and C,	3 take A, C, D,
	4 take B and D,	2 take all four,
	3 take C and D,	71 take none.

Let T be the number of students who take at least one course. By the inclusion–exclusion principle (Theorem 6.7),

$$T = s_1 - s_2 + s_3 - s_4, \text{ where}$$
$$s_1 = 12 + 20 + 20 + 8 = 60, \quad s_2 = 5 + 7 + 4 + 16 + 4 + 3 = 39$$
$$s_3 = 3 + 2 + 2 + 3 = 10, \quad s_4 = 2$$

Thus $T = 29$, and $N = 71 + T = 100$.

6.29. Prove that if A and B are disjoint finite sets, $A \cup B$ is finite and that

$$n(A \cup B) = n(A) + n(B)$$

In counting the elements of $A \cup B$, first count those that are in A. There are $n(A)$ of these. The only other elements of $A \cup B$ are those that are in B but not in A. But since A and B are disjoint, no element of B is in A, so there are $n(B)$ elements that are in B but not in A. Therefore, $n(A \cup B) = n(A) + n(B)$.

6.30. Prove Theorem 6.7 for two sets: $n(A \cup B) = n(A) + n(B) - n(A \cap B)$.

In counting the elements of $A \cup B$ we count the elements in A and count the elements in B. There are $n(A)$ in A and $n(B)$ in B. However, the elements $A \cap B$ were counted twice. Thus

$$n(A \cup B) = n(A) + n(B) - n(A \cap B)$$

as required. Alternately, we have the disjoint unions

$$A \cup B = A \cup (B \setminus A) \text{ and } B = (A \cap B) \cup (B \setminus A)$$

Therefore, according to the previous problem

$$n(A \cup B) = n(A) + n(B \setminus A) \text{ and } n(B) = n(A \cap B) + n(B \setminus A)$$

Thus $n(B \setminus A) = n(B) - n(A \cap B)$ and hence

$$n(A \cup B) = n(A) + n(B) - n(A \cap B)$$

as required.

Supplementary Problems

FACTORIAL NOTATION

6.31. Simplify: (*a*) $\dfrac{n+1)!}{n!}$; (*b*) $\dfrac{n!}{(n-2)!}$; (*c*) $\dfrac{(n-1)!}{(n+2)!}$; (*d*) $\dfrac{(n-r+1)!}{(n-r-1)!}$.

6.32. Evaluate: (*a*) $\binom{5}{2}$; (*b*) $\binom{7}{3}$; (*c*) $\binom{14}{2}$; (*d*) $\binom{6}{4}$; (*e*) $\binom{20}{17}$; (*f*) $\binom{18}{15}$.

PERMUTATIONS

6.33. Show that: (*a*) $\binom{n}{0}+\binom{n}{1}+\binom{n}{2}+\binom{n}{3}+\cdots+\binom{n}{n}=2^n$;

(*b*) $\binom{n}{0}-\binom{n}{1}+\binom{n}{2}-\binom{n}{3}+\cdots+\binom{n}{n}=0$.

6.34. (*a*) How many automobile license plates can be made if each plate contains two different letters followed by three different digits?

(*b*) Solve the problem if the first digit cannot be 0.

6.35. There are six roads between A and B and four roads between B and C. Find the number of ways that one can drive: (*a*) from A to C by way of B; (*b*) round-trip from A to C by way of B; (*c*) round-trip from A to C by way of B without using the same road more than once.

6.36. Find the number of ways in which six people can ride a toboggan if one of a subset of three must drive.

6.37. (*a*) Find the number of ways in which five persons can sit in a row.

(*b*) How many ways are there if two of the persons insist on sitting next to one another?

(*c*) Solve part (*a*) assuming they sit around a circular table.

(*d*) Solve part (*b*) assuming they sit around a circular table.

6.38. Find the number of ways in which five large books, four medium-size books, and three small books can be placed on a shelf so that all books of the same size are together.

6.39. (*a*) Find the number of permutations that can be formed from the letters of the word ELEVEN.

(*b*) How many of them begin and end with E?

(*c*) How many of them have the three Es together?

(*d*) How many begin with E and end with N?

6.40. (*a*) In how many ways can three boys and two girls sit in a row?

(*b*) In how many ways can they sit in a row if the boys and girls are each to sit together?

(*c*) In how many ways can they sit in a row if just the girls are to sit together?

COMBINATIONS

6.41. A woman has 11 close friends.

(*a*) In how many ways can she invite five of them to dinner?

(*b*) In how many ways if two of the friends are married and will not attend separately?

(*c*) In how many ways if two of them are not on speaking terms and will not attend together?

6.42. A woman has 11 close friends of whom six are also women.

(*a*) In how many ways can she invite three or more to a party?

(*b*) In how many ways can she invite three or more of them if she wants the same number of men as women (including herself)?

6.43. A student is to answer 10 out of 13 questions on an exam.

(*a*) How many choices has he?

(*b*) How many if he must answer the first two questions?

(*c*) How many if he must answer the first or second question but not both?

(*d*) How many if he must answer exactly three out of the first five questions?

(*e*) How many if he must answer at least three of the first five questions?

PARTITIONS

6.44. In how many ways can 10 students be divided into three teams, one containing four students and the others three?

6.45. In how many ways can 14 people be partitioned into six committees where two of the committees contain three members and the others two?

6.46. (*a*) Assuming that a cell can be empty, in how many ways can a set with three elements be partitioned into (i) three ordered cells, (ii) three unordered cells?

(*b*) In how many ways can a set with four elements be partitioned into (i) three ordered cells, (ii) three unordered cells?

MISCELLANEOUS PROBLEMS

6.47. A sample of 80 car owners revealed that 24 owned station wagons and 62 owned cars which are not station wagons. Find the number k of people who owned both a station wagon and some other car.

6.48. Suppose 12 people read the *Wall Street Journal (W)* or *Business Week (B)* or both. Given three people read only the *Journal* and six read both, find the number k of people who read only *Business Week*.

6.49. Show that any set of seven distinct integers includes two integers, x and y, such that either $x + y$ or $x - y$ is divisible by 10.

6.50. Consider a tournament in which each of n players plays against every other player and each player wins at least once. Show that there are at least two players having the same number of wins.

Answers to Supplementary Problems

6.31. (*a*) $n + 1$; (*b*) $n(n-1) = n^2 - n$; (*c*) $1/[n(n+1)(n+2)]$; (*d*) $(n-r)(n-r+1)$.

6.32. (*a*) 10; (*b*) 35; (*c*) 91; (*d*) 15; (*e*) 1140; (*f*) 816.

6.33. *Hints*: (*a*) Expand $(1+1)^n$; (*b*) Expand $(1-1)^n$.

6.34. (*a*) $26 \cdot 25 \cdot 10 \cdot 9 \cdot 8 = 468\,000$; (*b*) $26 \cdot 25 \cdot 9 \cdot 9 \cdot 8 = 421\,200$.

6.35. (*a*) 24; (*b*) 576; (*e*) 360.

6.36. 360.

6.37. (*a*) 120; (*b*) 48; (*c*) 24; (*d*) 12.

6.38. $3!\,5!\,4!\,3! = 103\,680$.

6.39. (*a*) 120; (*b*) 24; (*c*) 24; (*d*) 12.

6.40. (*a*) 120; (*b*) 24; (*c*) 48.

6.41. (*a*) 462; (*b*) 210; (*c*) 252.

6.42. (*a*) $2^{11} - 1 - \binom{11}{2} - \binom{11}{2} = 1981$ or $\binom{11}{3} + \binom{11}{4} + \cdots + \binom{11}{11} = 1981$.

(*b*) $\binom{5}{5}\binom{6}{4} + \binom{5}{4}\binom{6}{3} + \binom{5}{3}\binom{6}{2} + \binom{5}{2}\binom{6}{1} = 325$.

6.43. (*a*) 286; (*b*) 165; (*c*) 110; (*d*) 80; (*e*) 276.

6.44. $\dfrac{10!}{4!\,3!\,3!} \cdot \dfrac{1}{2!} = 2100$ or $\binom{10}{4}\binom{5}{2} = 2100$.

6.45. $\dfrac{14!}{3!\,3!\,2!\,2!\,2!\,2!} \cdot \dfrac{1}{2!\,4!} = 3\,153\,150$.

6.46. (*a*) (i) $3^3 = 27$ (each element can be placed in any of the three cells).

(ii) The number of elements in the three cells can be distributed as follows:
(*a*) [{3}, {0}, {0}]; (*b*) [{2}, {1}, {0}]; (*c*) [{1}, {1}, {1}].
Thus, the number of partitions is $1 + 3 + 1 = 5$.

(*b*) (i) $3^4 = 81$.

(ii) The number of elements in the three cells can be distributed as follows:
(*a*) [{4}, {0}, {0}]; (*b*) [{3}, {1}, {0}]; (*c*) [{2}, {2}, {0}]; (*d*) [{2}, {1}, {1}].
Thus, the number of partitions is $1 + 4 + 3 + 6 = 14$.

6.47. By Theorem 6.7, $k = 62 + 24 - 80 = 6$.

6.48. Note $W \cup B = (W \setminus B) \cup (W \cap B) \cup (B \setminus W)$ and the union is disjoint. Thus $12 = 3 + 6 + k$ or $k = 3$.

6.49. Let $X = \{x_1, x_2, \ldots, x_7\}$ be a set of seven distinct integers and let r_i be the remainder when x_i is divided by 10. Consider the following partition of X:

$H_1 = \{x_i : r_i = 0\}$ $\quad$ $H_2 = \{x_i : r_i = 5\}$
$H_3 = \{x_i : r_i = 1 \text{ or } 9\}$ $\quad$ $H_4 = \{x_i : r_i = 2 \text{ or } 8\}$
$H_5 = \{x_i : r_i = 3 \text{ or } 7\}$ $\quad$ $H_6 = \{x_i : r_i = 4 \text{ or } 6\}$

There are six pigeonholes for seven pigeons. If x and y are in H_1, or in H_2, then both $x + y$ and $x - y$ are divisible by 10. If x and y are in one of the other four subsets, then either $x - y$ or $x + y$ is divisible by 10, but not both.

6.50. The number of wins for a player is at least 1 and at most $n - 1$. These $n - 1$ numbers correspond to $n - 1$ pigeonholes which cannot accommodate n player-pigeons. Thus, at least two players will have the same number of wins.

© The McGraw–Hill Companies, 2004

Chapter 7

Probability Theory

7.1 INTRODUCTION

Probability theory is a mathematical modeling of the phenomenon of chance or randomness. If a coin is tossed in a random manner, it can land heads or tails, but we do not know which of these will occur in a single toss. However, suppose we let s be the number of times heads appears when the coin is tossed n times. As n increases, the ratio $f = s/n$, called the *relative frequency* of the outcome, becomes more stable. If the coin is perfectly balanced, then we expect that the coin will land heads approximately 50% of the time or, in other words, the relative frequency will approach $\frac{1}{2}$. Alternatively, assuming the coin is perfectly balanced, we can arrrive at the value $\frac{1}{2}$ deductively. That is, any side of the coin is as likely to occur as the other; hence the chance of getting a head is 1 in 2 which means the probability of getting a head is $\frac{1}{2}$. Although the specific outcome on any one toss is unknown, the behavior over the long run is determined. This stable long-run behavior of random phenomena forms the basis of probability theory.

A probabilistic mathematical model of random phenomena is defined by assigning "probabilities" to all the possible outcomes of an experiment. The reliability of our mathematical model for a given experiment depends upon the closeness of the assigned probabilities to the actual limiting relative frequencies. This then gives rise to problems of testing and reliability, which form the subject matter of statistics and which lie beyond the scope of this text.

7.2 SAMPLE SPACE AND EVENTS

The set S of all possible outcomes of a given experiment is called the *sample space*. A particular outcome, i.e., an element in S, is called a *sample point*. An *event* A is a set of outcomes or, in other words, a subset of the sample space S. In particular, the set $\{a\}$ consisting of a single sample point $a \in S$ is called an *elementary event*. Furthermore, the empty set $\varnothing$ and S itself are subsets of S and so are events; $\varnothing$ is sometimes called the *impossible event* or the *null event*.

Since an event is a set, we can combine events to form new events using the various set operations:

(i) $A \cup B$ is the event that occurs iff A occurs *or* B occurs (or both).

(ii) $A \cap B$ is the event that occurs iff A occurs and B occurs.

(iii) A^c, the complement of A, also written $\bar{A}$, is the event that occurs iff A does *not* occur.

Two events A and B are called *mutually exclusive* if they are disjoint, that is, if $A \cap B = \varnothing$. In other words, A and B are mutually exclusive iff they cannot occur simultaneously. Three or more events are mutually exclusive if every two of them are mutually exclusive.

EXAMPLE 7.1

(*a*) ***Experiment***: Toss a die and observe the number (of dots) that appears on top.

The sample space S consists of the six possible numbers; that is,

$$S = \{1, 2, 3, 4, 5, 6\}$$

Let A be the event that an even number occurs, B that an odd number occurs, and C that a prime number occurs; that is, let

$$A = \{2, 4, 6\}, \qquad B = \{1, 3, 5\}, \qquad C = \{2, 3, 5\}$$

Then

$A \cup C = \{2, 3, 4, 5, 6\}$ is the event that an even or a prime number occurs.

$B \cap C = \{3, 5\}$ is the event that an odd prime number occurs.

$C^c = \{1, 4, 6\}$ is the event that a prime number does not occur.

Note that A and B are mutually exclusive: $A \cap B = \varnothing$. In other words, an even number and an odd number cannot occur simultaneously.

(*b*) ***Experiment***: Toss a coin three times and observe the sequence of heads (T) and tails (T) that appears.

The sample space S consists of the following eight elements:

$$S = \{\text{HHH, HHT, HTH, HTT, THH, THT, TTH, TTT}\}$$

Let A be the event that two or more heads appear consecutively, and B that all the tosses are the same; that is, let

$$A = \{\text{HHH, HHT, THH}\}. \qquad \text{and} \qquad B = \{\text{HHH, TTT}\}$$

Then $A \cap B = \{\text{HHH}\}$ is the elementary event in which only heads appear. The event that five heads appear is the empty set $\varnothing$.

(*c*) ***Experiment***: Toss a coin until a head appears, and then count the number of times the coin is tossed.

The sample space of this experiment is $S = \{1, 2, 3, \ldots\}$. Since every positive integer is an element of S, the sample space is infinite.

Remark: The sample space S in Example 7.1(*c*), as noted, is not finite. The theory concerning such samples space lies beyond the scope of this text. Thus, unless otherwise stated, all our sample spaces S shall be finite.

7.3 FINITE PROBABILITY SPACES

The following definition applies.

Definition: Let S be a finite sample space, say $S = \{a_1, a_2, \ldots, a_n\}$. A *finite probability space*, or *probability model*, is obtained by assigning to each point a_i in S a real number p_i, called the *probability* of a_i, satisfying the following properties:

(i) Each p_i is nonnegative, that is, $p_i \geq 0$.

(ii) The sum of the p_i is 1, that is, $p_1 + p_2 + \cdots + p_n = 1$.

The *probability* of an event A written $P(A)$, is then defined to be the sum of the probabilities of the points in A.

The singleton set $\{a_i\}$ is called an *elementary* event and, for notational convenience, we write $P(a_i)$ for $P(\{a_i\})$.

EXAMPLE 7.2 ***Experiment***: Let three coins be tossed and the number of heads observed. [Compare with the above Example 7.1(*b*).]

The sample space is $S = \{0, 1, 2, 3\}$. The following assignments on the elements of S defines a probability space:

$$P(0) = \tfrac{1}{8}, \qquad P(1) = \tfrac{3}{8}, \qquad P(2) = \tfrac{3}{8}, \qquad P(3) = \tfrac{1}{8}$$

That is, each probability is nonnegative, and the sum of the probabilities is 1. Let A be the event that at least one head appears, and let B be the event that all heads or all tails appear; that is, let $A = \{1, 2, 3\}$ and $B = \{0, 3\}$. Then, by definition,

$$P(A) = P(1) + P(2) + P(3) = \tfrac{3}{8} + \tfrac{3}{8} + \tfrac{1}{8} = \tfrac{7}{8} \qquad \text{and} \qquad P(B) = P(0) + P(3) = \tfrac{1}{8} + \tfrac{1}{8} = \tfrac{1}{4}$$

Equiprobable Spaces

Frequently, the physical characteristics of an experiment suggest that the various outcomes of the sample space be assigned equal probabilities. Such a finite probability space S, where each sample point has the same probability, will be called an *equiprobable space*. In particular, if S contains n points, then the probability of each point is $1/n$. Furthermore, if an event A contains r points, then its probability is $r(1/n) = r/n$. In other words,

$$P(A) = \frac{\text{number of elements in } A}{\text{number of elements in } S} = \frac{n(A)}{n(S)} \qquad \text{or} \qquad P(A) = \frac{\text{number of outcomes favorable to } A}{\text{total number of possible outcomes}}$$

where $n(A)$ denotes the number of elements in a set A.

We emphasize that the above formula for $P(A)$ can only be used with respect to an equiprobable space, and cannot be used in general.

The expression *at random* will be used only with respect to an equiprobable space; the statement "choose a point at random from a set S" shall mean that every sample point in S has the same probability of being chosen.

EXAMPLE 7.3 Let a card be selected from an ordinary deck of 52 playing cards. Let

$$A = \{\text{the card is a spade}\} \qquad \text{and} \qquad B = \{\text{the card is a face card}\}$$

(A face card is a jack, queen, or king.) We compute $P(A)$, $P(B)$, and $P(A \cap B)$. Since we have an equiprobable space,

$$P(A) = \frac{\text{number of spades}}{\text{number of cards}} = \frac{13}{52} = \frac{1}{4}, \qquad P(B) = \frac{\text{number of face cards}}{\text{number of cards}} = \frac{12}{52} = \frac{3}{13}$$

$$P(A \cap B) = \frac{\text{number of spade face cards}}{\text{number of cards}} = \frac{3}{32}$$

Theorems on Finite Probability Spaces

The following theorem follows directly from the fact that the probability of an event is the sum of the probabilities of its points.

Theorem 7.1: The probability function P defined on the class of all events in a finite probability space has the following properties:

$[\mathbf{P}_1]$ For every event A, $0 \leq P(A) \leq 1$.
$[\mathbf{P}_2]$ $P(S) = 1$.
$[\mathbf{P}_3]$ If events A and B are mutually exclusive, then $P(A \cup B) = P(A) + P(B)$.

The next theorem formalizes our intuition that if p is the probability that an event E occurs, then $1 - p$ is the probability that E does not occur. (That is, if we hit a target $p = 1/3$ of the times, then we miss the target $1 - p = 2/3$ of the times.)

Theorem 7.2: Let A be any event. Then $P(A^c) = 1 - P(A)$.

The following theorem (proved in Problem 7.16) follows directly from Theorem 7.1.

Theorem 7.3: Let $\varnothing$ be the empty set, and suppose A and B are any events. Then:

(i) $P(\varnothing) = 0$.
(ii) $P(A \setminus B) = P(A) - P(A \cap B)$.
(iii) If $A \subseteq B$, then $P(A) \leq P(B)$.

Observe that Property $[\mathbf{P}_3]$ in Theorem 7.1 gives the probability of the union of events in the case that the events are disjoint. The general formula (proved in Problem 7.17) is called the Addition Principle. Specifically:

Theorem 7.4 (Addition Principle): For any events A and B,

$$P(A \cup B) = P(A) + P(B) - P(A \cap B)$$

EXAMPLE 7.4 Suppose a student is selected at random from 100 students where 30 are taking mathematics, 20 are taking chemistry, and 10 taking mathematics and chemistry. Find the probability p that the student is taking mathematics or chemistry.

Let $M = \{\text{students taking mathematics}\}$ and $C = \{\text{students taking chemistry}\}$. Since the space is equiprobable,

$$P(M) = \frac{30}{100} = \frac{3}{10} \qquad P(C) = \frac{20}{100} = \frac{1}{5}, \qquad P(M \text{ and } C) = P(M \cap C) = \frac{10}{100} = \frac{1}{10}$$

Thus, by the Addition Principle (Theorem 7.4),

$$p = P(M \text{ or } C) = P(M \cup C) = P(M) + P(C) - P(M \cap C) = \frac{3}{10} + \frac{1}{5} = \frac{1}{10} = \frac{2}{5}$$

7.4 CONDITIONAL PROBABILITY

Suppose E is an event in a sample space S with $P(E) > 0$. The probability that an event A occurs once E has occurred or, specifically, the *conditional probability of A given E*, written $P(A \mid E)$, is defined as follows:

$$P(A \mid E) = \frac{P(A \cap E)}{P(E)}$$

As pictured in the Venn diagram in Fig. 7-1, $P(A \mid E)$ measures, in a certain sense, the relative probability of A with respect to the reduced space E.

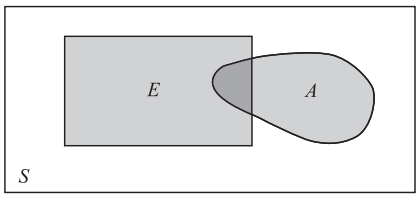


Fig. 7-1

Now suppose S is an equiprobable space, and we let $n(A)$ denote the number of elements in the event A. Then

$$P(A \cap E) = \frac{n(A \cap E)}{n(S)}, \qquad P(E) = \frac{n(E)}{n(S)}, \qquad \text{and so} \qquad P(A \mid E) = \frac{P(A \cap E)}{P(E)} = \frac{n(A \cap E)}{n(E)}$$

We state this result formally.

Theorem 7.5: Suppose S is an equiprobable space and A and B are events. Then

$$P(A \mid E) = \frac{\text{number of elements in } A \cap E}{\text{number of elements in } E} = \frac{n(A \cap E)}{n(E)}$$

EXAMPLE 7.5

(*a*) A pair of fair dice is tossed. The sample space S consists of the 36 ordered pairs (a, b) where a and b can be any of the integers from 1 to 6. (See Problem 7.3.) Thus the probability of any point is 1/36. Find the probability that one of the dice is 2 if the sum is 6. That is, find $P(A \mid E)$ where

$$E = \{\text{ sum is } 6\} \qquad \text{and} \qquad A = \{2 \text{ appears on at least one die}\}$$

Also find $P(A)$.

Now E consists of five elements, specifically

$$E = \{(1,5),\ (2,4),\ (3,3),\ (4,2),\ (5,1)\}$$

Two of them, $(2,4)$ and $(4,2)$, belong to A; that is,

$$A \cap E = \{(2,4),\ (4,2)\}$$

By Theorem 7.5, $P(A \mid E) = 2/5$.

On the other hand, A consists of 11 elements, specifically,

$$A = \{(2,1),\ (2,2),\ (2,3),\ (2,4),\ (2,5),\ (2,6),\ (1,2),\ 3,2),\ (4,2),\ (5,2),\ (6,2)\}$$

and S consists of 36 elements. Hence $P(A) = 11/36$.

(*b*) A couple has two children; the sample space is $S = \{bb, bg, gb, gg\}$ with probability 1/4 for each point. Find the probability p that both children are boys if it is known that: (i) at least one of the children is a boy, (ii) the older child is a boy.

(i) Here the reduced space consists of three elements, $\{bb, bg, gb\}$; hence $p = \frac{1}{3}$.

(ii) Here the reduced space consists of only two elements $\{bb, bg\}$; hence $p = \frac{1}{2}$.

Multiplication Theorem for Conditional Probability

Suppose A and B are events in a sample space S with $P(A) > 0$. By definition of conditional probability,

$$P(B \mid A) = \frac{P(A \cap B)}{P(A)}$$

Multiplying both sides by $P(A)$ gives us the following useful result:

Theorem 7.6 (Multiplication Theorem for Conditional Probability):

$$P(A \cap B) = P(A)P(B \mid A)$$

The multiplication theorem gives us a formula for the probability that events A and B both occur. It can easily be extended to three or more events $A_1, A_2, \ldots A_m$; that is,

$$P(A_1 \cap A_2 \cap \cdots \cap A_m) = P(A_1) \cdot P(A_2 \mid A_1) \cdot \cdots \cdot P(A_m \mid A_1 \cap A_2 \cap \cdots \cap A_{m-1})$$

EXAMPLE 7.6 A lot contains 12 items of which four are defective. Three items are drawn at random from the lot one after the other. Find the probability p that all three are nondefective.

The probability that the first item is nondefective is $\frac{8}{12}$ since eight of 12 items are nondefective. If the first item is nondefective, then the probability that the next item is nondefective is $\frac{7}{11}$ since only seven of the remaining 11 items are nondefective. If the first two items are nondefective, then the probability that the last item is nondefective is $\frac{6}{10}$ since only 6 of the remaining 10 items are now nondefective. Thus by the multiplication theorem,

$$p = \frac{8}{12} \cdot \frac{7}{11} \cdot \frac{6}{10} = \frac{14}{55} \approx 0.25$$

7.5 INDEPENDENT EVENTS

Events A and B in a probability space S are said to be *independent* if the occurrence of one of them does not influence the occurrence of the other. More specifically, B is independent of A if $P(B)$ is the same as $P(B \mid A)$. Now substituting $P(B)$ for $P(B \mid A)$ in the Multiplication Theorem $P(A \cap B) = P(A)P(B \mid A)$ yields

$$P(A \cap B) = P(A)P(B).$$

We formally use the above equation as our definition of independence.

Definition: Events A and B are *independent* if $P(A \cap B) = P(A)P(B)$; otherwise they are *dependent*.

We emphasize that independence is a symmetric relation. In particular, the equation

$$P(A \cap B) = P(A)P(B) \qquad \text{implies both} \qquad P(B \mid A) = P(B) \qquad \text{and} \qquad P(A \mid B) = P(A)$$

EXAMPLE 7.7 A fair coin is tossed three times yielding the equiprobable space

$$S = \{\text{HHH, HHT, HTH, HTT, THH, THT, TTH, TTT}\}$$

Consider the events:

$$A = \{\text{first toss is heads}\} = \{\text{HHH, HHT, HTH, HTT}\}$$
$$B = \{\text{second toss is heads}\} = \{\text{HHH, HHT, THH, THT}\}$$
$$C = \{\text{exactly two heads in a row}\} = \{\text{HHT, THH}\}$$

Clearly A and B are independent events; this fact is verified below. On the other hand, the relationship between A and C or B and C is not obvious. We claim that A and C are independent, but that B and C are dependent. We have

$$P(A) = \tfrac{4}{8} = \tfrac{1}{2}, \qquad P(B) = \tfrac{4}{8} = \tfrac{1}{2}, \qquad P(C) = \tfrac{2}{8} = \tfrac{1}{4}$$

Also,

$$P(A \cap B) = P(\{\text{HHH, HHT}\}) = \tfrac{1}{4}, \qquad P(A \cap C) = P(\{\text{HHT}\}) = \tfrac{1}{8}) \qquad P(B \cap C) = P(\{\text{HHT, THH}\}) = \tfrac{1}{4}$$

Accordingly,

$$P(A)P(B) = \tfrac{1}{2} \cdot \tfrac{1}{2} = \tfrac{1}{4} = P(A \cap B), \qquad \text{and so } A \text{ and } B \text{ are independent}$$
$$P(A)P(C) = \tfrac{1}{2} \cdot \tfrac{1}{4} = \tfrac{1}{8} = P(A \cap C), \qquad \text{and so } A \text{ and } C \text{ are independent}$$
$$P(B)P(C) = \tfrac{1}{2} \cdot \tfrac{1}{4} = \tfrac{1}{8} \neq P(B \cap C), \qquad \text{and so } B \text{ and } C \text{ are dependent}$$

Frequently, we will postulate that two events are independent, or the experiment itself will imply that two events are independent.

EXAMPLE 7.8 The probability that A hits a target is $\frac{1}{4}$, and the probability that B hits the target is $\frac{2}{5}$. Both shoot at the target. Find the probability that at least one of them hits the target, i.e., that A or B (or both) hit the target.

We are given that $P(A) = \frac{1}{4}$ and $P(B) = \frac{2}{5}$, and we seek $P(A \cup B)$. Furthermore, the probability that A or B hits the target is not influenced by what the other does; that is, the event that A hits the target is independent of the event that B hits the target, that is, $P(A \cap B) = P(A)P(B)$. Thus

$$P(A \cup B) = P(A) + P(B) - P(A \cap B) = P(A) + P(B) - P(A)P(B) = \tfrac{1}{4} + \tfrac{2}{5} - \left(\tfrac{1}{4}\right)\left(\tfrac{2}{5}\right) = \tfrac{11}{20}$$

7.6 INDEPENDENT REPEATED TRIALS, BINOMIAL DISTRIBUTION

We have previously discussed probability spaces which were associated with an experiment repeated a finite number of times, as the tossing of a coin three times. This concept of repetition is formalized as follows:

Definition: Let S be a finite probability space. By the space of *n independent repeated trials*, we mean the probability space S_n consisting of ordered n-tuples of elements of S, with the probability of an n-tuple defined to be the product of the probabilities of its components:

$$P((s_1, s_2, \cdots, s_n)) = P(s_1)P(s_2) \cdots P(s_n)$$

EXAMPLE 7.9 Whenever three horses a, b, and c race together, their respective probabilities of winning are $\frac{1}{2}$, $\frac{1}{3}$, and $\frac{1}{6}$. In other words, $S = \{a, b, c\}$ with $P(a) = \frac{1}{2}$, $P(b) = \frac{1}{3}$, and $P(c) = \frac{1}{6}$. If the horses race twice, then the sample space of the two repeated trials is

$$S_2 = \{aa, ab, ac, ba, bb, bc, ca, cb, cc\}$$

For notational convenience, we have written ac for the ordered pair (a, c). The probability of each point in S_2 is

$$P(aa) = P(a)P(a) = \tfrac{1}{2}\left(\tfrac{1}{2}\right) = \tfrac{1}{4}, \qquad P(ba) = \tfrac{1}{6}, \qquad P(ca) = \tfrac{1}{12}$$
$$P(ab) = P(a)P(b) = \tfrac{1}{2}\left(\tfrac{1}{3}\right) = \tfrac{1}{6}, \qquad P(bb) = \tfrac{1}{9}, \qquad P(cb) = \tfrac{1}{18}$$
$$P(ac) = P(a)P(c) = \tfrac{1}{2}\left(\tfrac{1}{6}\right) = \tfrac{1}{12}, \qquad P(bc) = \tfrac{1}{18}, \qquad P(cc) = \tfrac{1}{36}$$

Thus the probability of c winning the first race and a winning the second race is $P(ca) = \frac{1}{12}$.

Repeated Trials with Two Outcomes, Bernoulli Trials

Now consider an experiment with only two outcomes. Independent repeated trials of such an experiment are called Bernoulli trials, named after the Swiss mathematician Jacob Bernoulli (1654–1705). The term independent trials means that the outcome of any trial does not depend on the previous outcomes (such as, tossing a coin). We will call one of the outcomes *success* and the other outcome *failure*.

Let p denote the probability of success in a Bernoulli trial, and so $q = 1 - p$ is the probability of failure. A *binomial experiment* consists of a fixed number of Bernoulli trials. The notation

$$B(n, p)$$

will be used to denote a binomial experiment with n trials and probability p of success.

Frequently, we are interested in the number of successes in a binomial experiment and not in the order in which they occur. The following theorem (proved in Problem 7.38) applies.

Theorem 7.7: The probability of exactly k success in a binomial experiment $B(n, p)$ is given by

$$P(k) = P(k \text{ successes}) = \binom{n}{k} p^k q^{n-k}$$

The probability of one or more successes is $1 - q^n$.

Here $\binom{n}{k}$ is the binomial coefficient, which is defined and discussed in Chapter 6.

EXAMPLE 7.10 A fair coin is tossed 6 times; call heads a success. This is a binomial experiment with $n = 6$ and $p = q = \frac{1}{2}$.

(*a*) The probability that exactly two heads occurs (i.e., $k = 2$) is

$$P(2) = \binom{6}{2}\left(\frac{1}{2}\right)^2\left(\frac{1}{2}\right)^4 = \frac{15}{64} \approx 0.23$$

(*b*) The probability of getting at least four heads (i.e., $k = 4$, 5 or 6) is

$$P(4) + P(5) + P(6) = \binom{6}{4}\left(\frac{1}{2}\right)^4\left(\frac{1}{2}\right)^2 + \binom{6}{5}\left(\frac{1}{2}\right)^5\left(\frac{1}{2}\right) + \binom{6}{6}\left(\frac{1}{2}\right)^6$$
$$= \frac{15}{64} + \frac{6}{64} + \frac{1}{64} = \frac{11}{32} \approx 0.34$$

(*c*) The probability of getting no heads (i.e., all failures) is $q^6 = \left(\frac{1}{2}\right)^6 = \frac{1}{64}$, so the probability of one or more heads is $1 - q^n = 1 - \frac{1}{64} = \frac{63}{64} \approx 0.94$.

Remark: The function $P(k)$ for $k = 0, 1, 2, \ldots, n$, for a binomial experiment $B(n, p)$, is called the *binomial distribution* since it corresponds to the successive terms of the binomial expansion:

$$(q+p)^n = q^n + \binom{n}{1} q^{n-1}p + \binom{n}{2} q^{n-2}p^2 + \cdots + p^n$$

The use of the term *distribution* will be explained later in the chapter.

7.7 RANDOM VARIABLES

Let S be a sample of an experiment. As noted previously, the outcome of the experiment, or the points in S, need not be numbers. For example, in tossing a coin the outcomes are H (heads) or T (tails), and in tossing a pair of dice the outcomes are pairs of integers. However, we frequently wish to assign a specific number to each outcome of the experiment. For example, in coin tossing, it may be convenient to assign 1 to H and 0 to T; or, in the tossing of a pair of dice, we may want to assign the sum of the two integers to the outcome. Such an assignment of numerical values is called a *random variable*. More generally, we have the following definition.

Definition: A *random variable* X is a rule that assigns a numerical value to each outcome in a sample space S.

We shall let R_X denote the set of numbers assigned by a random variable X, and we shall refer to R_X as the *range space*.

Remark: In more formal terminology, X is a function from S to the real numbers $\mathbf{R}$, and R_X is the range of X. Also, for some infinite sample spaces S, not all functions from S to $\mathbf{R}$ are considered to be random variables. However, the sample spaces here are finite, and every real-valued function defined on a finite sample space is a random variable.

EXAMPLE 7.11 A pair of fair dice is tossed. (See Problem 7.3.) The sample space S consists of the 36 ordered pairs (a, b) where a and b can be any integers between 1 and 6; that is,

$$S = \{(1,1),\ (1,2), \ldots, (6,6)\}$$

Let X assign to each point in S the sum of the numbers; then X is a random variable with range space

$$R_X = \{2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$$

Let Y assign to each point the maximum of the two numbers; then Y is a random variable with range space

$$R_Y = \{1, 2, 3, 4, 5, 6\}$$

EXAMPLE 7.12 A box contains 12 items of which three are defective. A sample of three items is selected from the box. The sample space S consists of the $\binom{12}{3} = 220$ different samples of size 3. Let X denote the number of defective items in the sample; then X is a random variable with range space $R_X = \{0, 1, 2, 3\}$.

Probability Distribution of a Random Variable

Let $R_X = \{x_1, x_2, \ldots, x_t\}$ be the range space of a random variable X defined on a finite sample space S. Then X induces an assignment of probabilities on the range space R_X as follows:

$$p_i = P(x_i) = P(X = x_i) = \text{sum of probabilities of points in } S \text{ whose image is } x_i$$

The set of ordered pairs $(x_1, p_1), \ldots, (x_t, p_t)$, usually given by a table

x_1	x_2	$\cdots$	x_t
p_1	p_2	$\cdots$	p_t

is called the *distribution* of the random variable X.

In the case that S is an equiprobable space, we can easily obtain the distribution of a random variable from the following result.

Theorem 7.8: Let S be an equiprobable space, and let X be a random variable on S with range space

$$R_X = \{x_1, x_2, \ldots, x_t\}.$$

Then

$$p_i = P(x_i) = \frac{\text{number of points in } S \text{ whose image is } x_i}{\text{number of points in } S}$$

EXAMPLE 7.13 Consider the random variable X in Example 7.11 which assigns the sum to the toss of a pair of dice. We use Theorem 7.8 to obtain the distribution of X.

There is only one outcome $(1,1)$ whose sum is 2; hence $P(2) = \frac{1}{36}$. There are two outcomes, $(1,2)$ and $(2,1)$, whose sum is 3; hence $P(3) = \frac{2}{36}$. There are three outcomes, $(1,3)$, $(2,2)$, $(3,1)$, whose sum is 4; hence $P(4) = \frac{3}{36}$. Similarly $P(5) = \frac{4}{36}$, $P(6) = \frac{5}{36}, \ldots, P(12) = \frac{1}{36}$. The distribution of X consists of the points in R_X with their respective probabilities; that is,

x_i	2	3	4	5	6	7	8	9	10	11	12
p_i	$\frac{1}{36}$	$\frac{2}{36}$	$\frac{3}{36}$	$\frac{4}{36}$	$\frac{5}{36}$	$\frac{6}{36}$	$\frac{5}{36}$	$\frac{4}{36}$	$\frac{3}{36}$	$\frac{2}{36}$	$\frac{1}{36}$

EXAMPLE 7.14 Let X be the random variable in Example 7.12. We use Theorem 7.8 to obtain the distribution of X.

There are $\binom{9}{3} = 84$ samples of size 3 with no defective items; hence $P(0) = \frac{84}{220}$. There are $3\binom{9}{2} = 108$ samples of size 3 containing one defective item; hence $P(1) = \frac{108}{220}$. There are $\binom{3}{2} \cdot 9 = 27$ samples of size 3 containing two defective items; hence $P(2) = \frac{27}{220}$. There is only one sample of size 3 containing the three defective items; hence $P(3) = \frac{1}{220}$. The distribution of X follows:

x_i	0	1	2	3
p_i	$\frac{84}{220}$	$\frac{108}{220}$	$\frac{27}{220}$	$\frac{1}{220}$

Remark: Let X be a random variable on a probability space $S = \{a_1, a_2, \ldots, a_m\}$, and let $f(x)$ be any polynomial. Then $f(X)$ is the random variable which assigns $f(X(a_i))$ to the point a_i or, in other words, $f(X)(a_i) = f(X(a_i))$. Accordingly, if X takes on the values $x_1, x_2, \ldots, x_n$ with respective probabilities $p_1, p_2, \ldots, p_n$, then $f(X)$ takes on the values $f(x_1), f(x_2), \ldots, f(x_n)$ where the probability q_k of y_k is the sum of those p_i's for which $y_k = f(x_i)$.

Expectation of a Random Variable

Let X be a random variable. There are two important measurements (or parameters) associated with X, the *mean* of X, denoted by μ or μ_X, and the *standard deviation* of X denoted by σ or σ_X. The mean μ is also called the *expectation* of X, written $E(X)$. In a certain sense, the mean μ measures the "central tendency" of X, and the standard deviation σ measures the "spread" or "dispersion" of X. (The mean is sometimes called the *average* value since it corresponds to the average of a set of numbers where the probability of a number is defined by the relative frequency of the number in the set.) This subsection discusses the expectation $\mu = E(X)$ of X, and the next subsection discusses the standard deviation σ of X.

Let X be a random variable on a probability space $S = \{a_1, a_2, \cdots, a_m\}$. The *mean* or *expectation* of X is defined by

$$\mu = E(X) = X(a_1)P(a_1) + X(a_2)P(a_2) + \cdots + X(a_m)P(a_m) = \Sigma X(a_i)P(a_i)$$

In particular, if X is given by the distribution

x_1	x_2	$\cdots$	x_n
p_1	p_2	$\cdots$	p_n

then the *expectation* of X is

$$\mu = E(X) = x_1p_1 + x_2p_2 + \cdots + x_np_n = \Sigma x_ip_i$$

(For notational convenience, we have omitted the limits in the summation symbol Σ.)

EXAMPLE 7.15

(*a*) Suppose a fair coin is tossed six times. The number of heads which can occur with their respective probabilities are as follows:

x_i	0	1	2	3	4	5	6
p_i	$\frac{1}{64}$	$\frac{6}{64}$	$\frac{15}{64}$	$\frac{20}{64}$	$\frac{15}{64}$	$\frac{6}{64}$	$\frac{1}{64}$

Then the mean or expectation or expected number of heads is

$$\mu = E(X) = 0\left(\tfrac{1}{64}\right) + 1\left(\tfrac{6}{64}\right) + 2\left(\tfrac{15}{64}\right) + 3\left(\tfrac{20}{64}\right) + 4\left(\tfrac{15}{64}\right) + 5\left(\tfrac{6}{64}\right) + 6\left(\tfrac{1}{64}\right) = 3$$

(*b*) Consider the random variable X in Example 7.12 whose distribution appears in Example 7.14. It gives the possible numbers of defective items in a sample of size 3 with their respective probabilities. Then the expectation of X or, in other words, the expected number of defective items in a sample of size 3, is

$$\mu = E(X) = 0\left(\tfrac{84}{220}\right) + 1\left(\tfrac{108}{220}\right) + 2\left(\tfrac{27}{220}\right) + 3\left(\tfrac{1}{220}\right) = 0.75$$

(*c*) Three horses a, b, and c are in a race; suppose their respective probabilities of winning are $\frac{1}{2}$, $\frac{1}{3}$, and $\frac{1}{6}$. Let X denote the payoff function for the winning horse, and suppose X pays \$2, \$6, or \$9 according as a, b, or c wins the race. The expected payoff for the race is

$$\begin{aligned} E(X) &= X(a)P(a) + X(b)P(b) + X(c)P(c) \\ &= 2\left(\tfrac{1}{2}\right) + 6\left(\tfrac{1}{3}\right) + 9\left(\tfrac{1}{6}\right) = 4.5 \end{aligned}$$

Variance and Standard Deviation of a Random Variable

Consider a random variable X with mean μ and probability distribution

x_1	x_2	x_3	$\cdots$	x_n
p_1	p_2	p_3	$\cdots$	p_n

The *variance* $\mathrm{Var}(X)$ and *standard deviation* σ of X are defined by

$$\mathrm{Var}(X) = (x_1 - \mu)^2p_1 + (x_2 - \mu)^2p_2 + \cdots + (x_n - \mu)^2p_n = \Sigma(x_i - \mu)^2p_i = E((X - \mu)^2)$$

$$\sigma = \sqrt{\mathrm{Var}(X)}$$

The following formula is usually more convenient for computing $\mathrm{Var}(X)$ than the above:

$$\mathrm{Var}(X) = x_1^2p_1 + x_2^2p_2 + \cdots + x_n^2p_n - \mu^2 = \Sigma x_i^2p_i - \mu^2 = E(X^2) - \mu^2$$

Remark: According to the above formula, $\text{Var}(X) = \sigma^2$. Both σ^2 and σ measure the weighted spread of the values x_i about the mean μ; however, σ has the same units as μ.

EXAMPLE 7.16

(*a*) Let X denote the number of times heads occurs when a fair coin is tossed six times. The distribution of X appears in Example 7.15(*a*), where its mean $\mu = 3$ is computed. The variance of X is computed as follows:

$$\text{Var}(X) = (0-3)^2\tfrac{1}{64} + (1-3)^2\tfrac{6}{64} + (2-3)^2\tfrac{15}{64} + \cdots + (6-3)\tfrac{1}{64} = 1.5$$

Alternatively:

$$\text{Var}(X) = 0^2\tfrac{1}{64} + 1^2\tfrac{6}{64} + 2^2\tfrac{15}{64} + 3^2\tfrac{20}{64} + 4^2\tfrac{15}{64} + 5^2\tfrac{6}{64} + 6^2\tfrac{1}{64} - 3^2 = 1.5$$

Thus the standard deviation is $\sigma = \sqrt{1.5} \approx 1.225$ (heads).

(*b*) Consider the random variable X in Example 7.15(*b*), where its mean $\mu = 0.75$ is computed. (Its distribution appears in Example 7.14.) The variance of X is computed as follows:

$$\text{Var}(X) = 0^2\tfrac{84}{220} + 1^2\tfrac{108}{220} + 2^2\tfrac{27}{220} + 3^2\tfrac{1}{220} - (0.75)^2 = 0.46$$

Thus the standard deviation is

$$\sigma = \sqrt{\text{Var}(X)} = \sqrt{0.46} = 0.66$$

Binomial Distribution

Consider a binomial experiment $B(n, p)$. That is, $B(n, p)$ consists of n independent repeated trials with two outcomes, success or failure, and p is the probability of success. The number X of k successes is a random variable with distribution appearing in Fig. 7-2.

k	0	1	2	$\cdots$	n
$P(k)$	q^n	$\binom{n}{1}q^{n-1}p$	$\binom{n}{2}q^{n-2}p^2$	$\cdots$	p^n

Fig. 7-2

The following theorem applies.

Theorem 7.9: Consider the binomial distribution $B(n, p)$. Then:

(i) Expected value $E(X) = \mu = np$.
(ii) Variance $\text{Var}(X) = \sigma^2 = npq$.
(iii) Standard deviation $\sigma = \sqrt{npq}$.

EXAMPLE 7.17

(*a*) The probability that a man hits a target is $p = 1/5$. He fires 100 times. Find the expected number μ of times he will hit the target and the standard deviation σ.

Here $p = \frac{1}{5}$ and so $q = \frac{4}{5}$. Hence

$$\mu = np = 100 \cdot \frac{1}{5} = 20 \qquad \text{and} \qquad \sigma = \sqrt{npq} = \sqrt{100 \cdot \frac{1}{5} \cdot \frac{4}{5}} = 4$$

(*b*) Find the expected number $E(X)$ of correct answers obtained by guessing in a five-question true–false test.

Here $p = \frac{1}{2}$. Hence $E(X) = np = 5 \cdot \frac{1}{2} = 2.5$.

Solved Problems

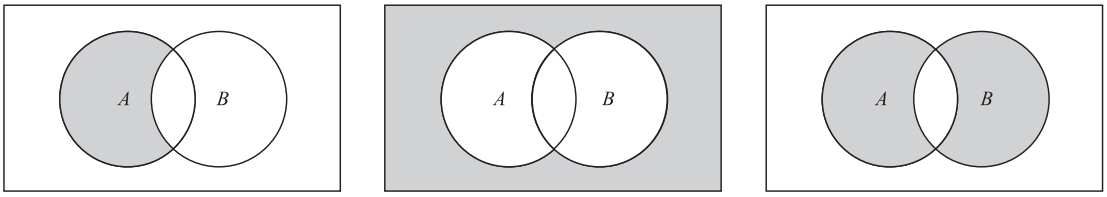
SAMPLE SPACES AND EVENTS

7.1. Let A and B be events. Find an expression and exhibit the Venn diagram for the events: (a) A but not B; (b) neither A nor B; (c) either A or B, but not both.

(a) Since A but not B occurs, shade the area of A outside of B, as in Fig. 7-3(a). Note that B^c, the complement of B, occurs, since B does not occur; hence A and B^c occur. In other words the event is $A \cap B^c$.

(b) "Neither A nor B" means "not A and not B", or $A^c \cap B^c$. By DeMorgan's law, this is also the set $(A \cup B)^c$; hence shade the area outside of A and B, i.e., outside $A \cup B$, as in Fig. 7-3(b).

(c) Since A or B, but not both, occurs, shade the area of A and B, except where they intersect, as in Fig. 7-3(c). The event is equivalent to the occurrence of A but not B or B but not A. Thus the event is $(A \cap B^c) \cup (B \cap A^c)$.



(a) A but not B (b) Neither A nor B (c) A or B, but not both

Fig. 7-3

7.2. Let a coin and a die be tossed; and let the sample space S consist of the 12 elements:

$$S = \{\text{H1, H2, H3, H4, H5, H6, T1, T2, T3, T4, T5, T6}\}$$

(a) Express explicitly the following events:

$$A = \text{ heads and an even number appears}\}$$

$$B = \{\text{a prime number appears}\}$$

$$C = \{\text{tails and an odd number appears}\}$$

(b) Express explicitly the events: (i) A or B occurs; (ii) B and C occur: (iii) only B occurs.

(c) Which pair of the events A, B, and C are mutually exclusive?

(a) The elements of A are those elements of S consisting of an H and an even number:

$$A = \{\text{H2, H4, H6}\}$$

The elements of B are those points in S whose second component is a prime number:

$$B = \{\text{H2, H3, H5, T2, T3, T5}\}$$

The elements of C are those points in S consisting of a T and an odd number: $C = \{\text{T1, T3, T5}\}$.

(b) (i) $A \cup B = \{\text{H2, H4, H6, H3, H5, T2, T3, T5}\}$.

(ii) $B \cap C = \{\text{T3, T5}\}$.

(iii) $B \cap A^c \cap C^c = \{\text{H3, H5, T2}\}$.

(c) A and C are mutually exclusive since $A \cap C = \varnothing$.

7.3. A pair of dice is tossed and the two numbers appearing on the top are recorded. Describe the sample space S, and find the number $n(S)$ of elements in S.

There are six possible numbers, 1, 2, ..., 6, on each die. Hence $n(S) = 6 \cdot 6 = 36$, and S consists of the 36 pairs of numbers from 1 to 6. Figure 7-4 shows these 36 pairs of numbers in an array where each row has the same first element and each column has the same second element.

$$\begin{array}{cccccc}
(1,1), & (1,2), & (1,3), & (1,4), & (1,5), & (1,6) \\
(2,1), & (2,2), & (2,3), & (2,4), & (2,5), & (2,6) \\
(3,1), & (3,2), & (3,3), & (3,4), & (3,5), & (3,6) \\
(4,1), & (4,2), & (4,3), & (4,4), & (4,5), & (4,6) \\
(5,1), & (5,2), & (5,3), & (5,4), & (5,5), & (5,6) \\
(6,1), & (6,2), & (6,3), & (6,4), & (6,5), & (6,6)
\end{array}$$

Fig. 7-4

7.4. Consider the sample space S in Problem 7.3. Find the number of elements in each of the following events:

(*a*) $A = \{\text{the two numbers are equal}\}$.

(*b*) $B = \{\text{the sum is 10 or more}\}$.

(*c*) $C = \{5 \text{ appears on the first die}\}$.

(*d*) $D = \{5 \text{ appears on at least one die}\}$.

(*e*) $E = \{\text{the sum is 7 or less}\}$.

Use Fig. 7-4 to help count the number of elements which are in the event:

(*a*) $A = \{(1,1), (2,2), \ldots, (6,6)\}$, so $n(A) = 6$.

(*b*) $B = \{(6,4), (5,5), (4,6), (6,5), (5,6), (6,6)\}$, so $n(B) = 6$.

(*c*) $C = \{(5,1), (5,2), \ldots, (5,6)$, so $n(C) = 6$.

(*d*) There are six pairs with 5 as the first element, and six pairs with 5 as the second element. However, $(5,5)$ appears in both places. Hence

$$n(D) = 6 + 6 - 1 = 11$$

Alternatively, count the pairs in Fig. 7-4 which are in D to get $n(D) = 11$.

(*e*) Let $n(s)$ denote the number of pairs in S where the sum is s. The sum 7 appear on the diagonal of the array in Fig. 7-4; hence $n(7) = 6$. The sum 6 appears directly below the diagonal, so $n(6) = 5$. Similarly, $n(5) = 4$, $n(4) = 3$, $n(3) = 2$, and $n(2) = 1$. Thus

$$n(S) = 6 + 5 + 4 + 3 + 2 + 1 = 21$$

Alternatively, $n(7) = 6$ and there are $36 - 6 = 30$ pairs remaining. Half of them have sums exceeding 7 and half of them have sums less than 7. Thus $n(s) = 6 + 15 = 21$.

FINITE EQUIPROBABLE SPACES

7.5. Determine the probability p of each event:

(*a*) An even number appears in the toss of a fair die.

(*b*) One or more heads appear in the toss of three fair coins.

(*c*) A red marble appears in random drawing of one marble from a box containing four white, three red, and five blue marbles.

Each sample space S is an equiprobable space. Hence, for each event E, use

$$P(E) = \frac{\text{number of elements in } E}{\text{number of elements in } S} = \frac{n(E)}{n(S)}$$

(*a*) The event can occur in three ways (2, 4 or 6) out of 6 cases; hence $p = \frac{3}{6} = \frac{1}{2}$.

(*b*) Assuming the coins are distinguished, there are 8 cases:

$$\text{HHH, HHT, HTH, HTT, THH, THT, TTH, TTT,}$$

Only the last case is not favorable; hence $p = 7/8$.

(*c*) There are $4 + 3 + 5 = 12$ marbles of which three are red; hence $p = \frac{3}{12} = \frac{1}{4}$.

7.6. A single card is drawn from an ordinary deck S of 52 cards. Find the probability p that:

(*a*) The card is a king.

(*b*) The card is a face card (jack, queen or king).

(*c*) The card is a heart.

(*d*) The card is a face card and a heart.

(*e*) The card is a face card or a heart.

Here $n(S) = 52$.

(*a*) There are four kings; hence $p = \frac{4}{52} = \frac{1}{13}$.

(*b*) There are $4(3) = 12$ face cards; hence $p = \frac{12}{52} = \frac{3}{13}$.

(*c*) There are 13 hearts; hence $p = \frac{13}{52} = \frac{1}{4}$.

(*d*) There are three face cards which are hearts; hence $p = \frac{3}{52}$.

(*e*) Letting $F = \{\text{face cards}\}$ and $H = \{\text{hearts}\}$, we have

$$n(F \cup H) = n(F) + n(H) - n(F \cap H) = 12 + 13 - 3 = 22$$

Hence $p = \frac{22}{52} = \frac{11}{26}$.

7.7. Consider the sample space S in Problem 7.2. Assume the coin and die are fair; hence S is an equiprobable space. Find: (*a*) $P(A)$, $P(B)$, $P(C)$; (*b*) $P(A\cup$

Since S is an equiprobable space, use $P(E) = n(E)/n(S)$. Here $n(S) = 12$. So we need only count the number of elements in the given set.

(*a*) $P(A) = \frac{3}{12}$, $P(B) = \frac{6}{12}$, $P(C) = \frac{3}{12}$.

(*b*) $P(A \cup B) = \frac{8}{12}$, $P(B \cap C) = \frac{2}{12}$, $P(B \cap A^c \cap C^c) = \frac{3}{12}$.

7.8. Two cards are drawn at random from an ordinary deck of 52 cards. Find the probability p that: (*a*) both are spades; (*b*) one is a spade and one is a heart.

There are $\binom{52}{2} = 1326$ ways to draw 2 cards from 52 cards.

(*a*) There are $\binom{13}{2} = 78$ ways to draw 2 spades from 13 spades; hence

$$p = \frac{\text{number of ways 2 spades can be drawn}}{\text{number of ways 2 cards can be drawn}} = \frac{78}{1326} = \frac{3}{51}$$

(*b*) There are 13 spades and 13 hearts, so there are $13 \cdot 13 = 169$ ways to draw a spade and a heart. Thus $p = \frac{169}{1326} = \frac{13}{102}$.

7.9. A box contains two white socks and two blue socks. Two socks are drawn at random. Find the probability p they are a match (same color).

There are $\binom{4}{2} = 6$ ways to draw two of the socks. Only two pairs will yield a match. Thus $p = \frac{2}{6} = \frac{1}{3}$.

7.10. Five horses are in a race. Audrey picks two of the horses at random, and bets on them. Find the probability p that Audrey picked the winner.

There are $\binom{5}{2} = 10$ ways to pick two of the horses. Four of the pairs will contain the winner. Thus $p = \frac{4}{10} = \frac{2}{5}$.

FINITE PROBABILITY SPACES

7.11. A sample space S consists of four elements; that is, $S = \{a_1, a_2, a_3, a_4\}$. Under which of the following functions does S become a probability space?

(*a*) $P(a_1) = \frac{1}{2}$ $P(a_2) = \frac{1}{3}$ $P(a_3) = \frac{1}{4}$ $P(a_4) = \frac{1}{5}$

(*b*) $P(a_1) = \frac{1}{2}$ $P(a_2) = \frac{1}{4}$ $P(a_3) = -\frac{1}{4}$ $P(a_4) = \frac{1}{2}$

(*c*) $P(a_1) = \frac{1}{2}$ $P(a_2) = \frac{1}{4}$ $P(a_3) = \frac{1}{8}$ $P(a_4) = \frac{1}{8}$

(*d*) $P(a_1) = \frac{1}{2}$ $P(a_2) = \frac{1}{4}$ $P(a_3) = \frac{1}{4}$ $P(a_4) = 0$

(*a*) Since the sum of the values on the sample points is greater than one, the function does not define S as a probability space.

(*b*) Since $P(a_3)$ is negative, the function does not define S as a probability space.

(*c*) Since each value is nonnegative and the sum of the values is one, the function does define S as a probability space.

(*d*) The values are nonnegative and add up to one; hence the function does define S as a probability space.

7.12. A coin is weighted so that heads is twice as likely to appear as tails. Find $P(T)$ and $P(H)$.

Let $P(T) = p$; then $P(H) = 2p$. Now set the sum of the probabilities equal to one, that is, set $p + 2p = 1$. Then $p = \frac{1}{3}$. Thus $P(H) = \frac{1}{3}$ and $P(T) = \frac{2}{3}$.

7.13. A die is weighted so that the outcomes produce the following probability distribution:

Outcome	1	2	3	4	5	6
Probability	0.1	0.3	0.2	0.1	0.1	0.2

Consider the events:

$A = \{\text{even number}\}$, $B = \{2, 3, 4, 5\}$, $C = \{x\colon x < 3\}$, $D = \{x\colon x > 7\}$

Find the following probabilities:

(*a*) (i) $P(A)$, (ii) $P(B)$, (iii) $P(C)$, (iv) $P(D)$.

(*b*) $P(A^c)$, $P(B^c)$, $P(C^c)$, $P(D^c)$.

(*c*) (i) $P(A \cap B)$, (ii) $P(A \cup C)$, (iii) $P(B \cap C)$.

(*a*) For any event, find $P(E)$ by summing the probabilities of the elements in E. Thus:
(i) $A = \{2, 4, 6\}$, so $P(A) = 0.3 + 0.1 + 0.2 = 0.6$.
(ii) $P(B) = 0.3 + 0.2 + 0.1 + 0.1 = 0.7$.
(iii) $C = \{1, 2\}$, so $P(C) = 0.1 + 0.3 = 0.4$.
(iv) $D = \varnothing$, the empty set. Hence $P(D) = 0$.

(*b*) Use $P(E^c) = 1 - P(E)$ to get:
$P(A^c) = 1 = 0.6 = 0.4, \qquad P(C^c) = 1 - 0.4 = 0.6$
$P(B^c) = 1 - 0.7 = 0.3, \qquad P(D^c) = 1 - 0 = 1$

(*c*) (i) $A \cap B = \{2, 4\}$, so $P(A \cap B) = 0.3 + 0.1 = 0.4$.
(ii) $A \cup C = \{1, 2, 3, 4, 5\} = \{6\}^c$, so $P(A \cup C) = 1 - 0.2 = 0.8$.
(iii) $B \cap C = \{2\}$, so $P(B \cap C) = 0.3$.

7.14. Suppose A and B are events with $P(A) = 0.6$, $P(B) = 0.3$, and $P(A \cap B) = 0.2$. Find the probability that:

(*a*) A does not occur. (*c*) A or B occurs.
(*b*) B does not occur. (*d*) Neither A nor B occurs.

(*a*) $P(\text{not } A) = P(A^c) = 1 - P(A) = 0.4$.
(*b*) $P(\text{not } B) = P(B^c) = 1 - P(B) = 0.7$.
(*c*) By the Addition Principle,

$$P(A \text{ or } B) = P(A \cup B) = P(A) + P(B) - P(A \cap B)$$
$$= 0.6 + 0.3 - 0.2 = 0.7$$

(*d*) Recall [Fig. 7-3(*b*)] that neither A nor B is the complement of $A \cup B$. Therefore,

$$P(\text{neither } A \text{ nor } B) = P((A \cup B)^c) = 1 - P(A \cup B) = 1 - 0.7 = 0.3$$

7.15. Prove Theorem 7.2: $P(A^c) = 1 - P(A)$.

$S = A \cup A^c$ where A and A^c are disjoint. Thus

$$1 = P(S) = P(A \cup A^c) = P(A) + P(A^c)$$

from which our result follows.

7.16. Prove Theorem 7.3: (i) $P(\varnothing) = 0$, (ii) $P(A \setminus B) = P(A) - P(A \cap B)$, (iii) If $A \subseteq B$, then $P(A) \leq P(B)$.

(i) $\varnothing = S^c$ and $P(S) = 1$. Thus $P(\varnothing) = 1 - 1 = 0$.

(ii) As indicated by Fig. 7-5(*a*), $A = (A \setminus B) \cup (A \cap B)$ where $A \setminus B$ and $A \cap B$ are disjoint. Hence

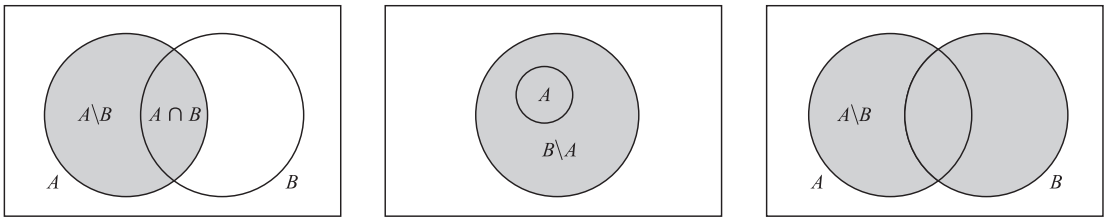
$$P(A) = P(A \setminus B) + P(A \cap B)$$

From which our result follows.

(iii) If $A \subseteq B$, then, as indicated by Fig. 7-5(*b*), $B = A \cup (B \setminus A)$ where A and $B \setminus A$ are disjoint. Hence

$$P(B) = P(A) + P(B \setminus A)$$

Since $P(B \setminus A) \geq 0$, we have $P(A) \leq P(B)$.



(*a*) A is shaded (*b*) B is shaded (*c*) $A \cup B$ is shaded

Fig. 7-5

7.17. Prove Theorem (Addition Principle) 7.4: For any events A and B,

$$P(A \cup B) = P(A) + P(B) - P(A \cap B)$$

As indicated by Fig. 7-5(*c*), $A \cup B = (A \setminus B) \cup B$ where $A \setminus B$ and B are disjoint sets. Thus, using Theorem 7.3(ii),

$$\begin{aligned} P(A \cup B) &= P(A \setminus B) + P(B) = P(A) - P(A \cap B) + P(B) \\ &= P(A) + P(B) - P(A \cap B) \end{aligned}$$

CONDITIONAL PROBABILITY

7.18. Three fair coins, a penny, a nickel, and a dime, are tossed. Find the probability p that they are all heads if: (*a*) the penny is heads; (*b*) at least one of the coins is heads.

The sample space has eight elements: $S = \{\text{HHH, HHT, HTH, HTT, THH, THT, TTH, TTT}\}$.

(*a*) If the penny is heads, the reduced sample space is $A = \{\text{HHH, HHT, HTH, HTT}\}$. Since the coins are all heads in 1 of 4 cases, $p = \frac{1}{4}$.

(*b*) If one or more of the coins is heads, the reduced sample space is

$$B = \{\text{HHH, HHT, HTH, HTT, THH, THT, TTH}\}.$$

Since the coins are all heads in 1 of 7 cases, $p = \frac{1}{7}$.

7.19. A pair of fair dice is thrown. Find the probability p that the sum is 10 or greater if: (*a*) 5 appears on the first die; (*b*) 5 appears on at least one die.

(*a*) If a 5 appears on the first die, then the reduced sample space is

$$A = \{(5,1),\ (5,2),\ (5,3),\ (5,4),\ (5,5),\ (5,6)\}$$

The sum is 10 or greater on two of the six outcomes: $(5,5),\ (5,6)$. Hence $p = \frac{2}{6} = \frac{1}{3}$.

(*b*) If a 5 appears on at least one of the dice, then the reduced sample space has eleven elements.

$$B = \{(5,1),\ (5,2),\ (5,3),\ (5,4),\ (5,5),\ (5,6),\ (1,5),\ (2,5),\ (3,5),\ (4,5),\ (6,5)\}$$

The sum is 10 or greater on three of the eleven outcomes: $(5,5),\ (5,6),\ (6,5)$. Hence $p = \frac{3}{11}$.

7.20. In a certain college town, 25% of the students failed mathematics, 15% failed chemistry, and 10% failed both mathematics and chemistry. A student is selected at random.

(*a*) If he failed chemistry, what is the probability that he failed mathematics?

(*b*) If he failed mathematics, what is the probability that he failed chemistry?

(*c*) What is the probability that he failed mathematics or chemistry?

(*d*) What is the probability that he failed neither mathematics nor chemistry?

(*a*) The probability that a student failed mathematics, given that he failed chemistry, is

$$P(M \mid C) = \frac{P(M \cap C)}{P(C)} = \frac{0.10}{0.15} = \frac{2}{3}$$

(*b*) The probability that a student failed chemistry, given that he failed mathematics is

$$P(C \mid M) = \frac{P(C \cap M)}{P(M)} = \frac{0.10}{0.25} = \frac{2}{5}$$

(*c*) By the Addition Principle (Theorem 7.4),

$$P(M \cup C) = P(M) + P(C) - P(M \cap C) = 0.25 + 0.15 - 0.10 = 0.30$$

(*d*) Students who failed neither mathematics nor chemistry form the complement of the set $M \cup C$, that is, they form the set $(M \cup C)^c$. Hence

$$P((M \cup C)^c) = 1 - P(M \cup C) = 1 - 0.30 = 0.70$$

7.21. A pair of fair dice is thrown. If the two numbers appearing are different, find the probability p that: (*a*) the sum is 6; (*b*) an ace appears; (*c*) the sum is 4 or less.

There are 36 ways the pair of dice can be thrown, and six of them, (1, 1), (2, 2), . . ., (6, 6), have the same numbers. Thus the reduced sample space will consist of $36 - 6 = 30$ elements.

(*a*) The sum 6 can appear in four ways: $(1,5), (2,4), (4,2), (5,1)$. (We cannot include $(3,3)$ since the numbers, are the same.) Hence $p = \frac{4}{30} = \frac{2}{15}$.

(*b*) An ace can appear in 10 ways: $(1,2), (1,3), \ldots, (1,6)$ and $(2,1), (3,1), \ldots, (6,1)$. Therefore $p = \frac{10}{30} = \frac{1}{3}$.

(*c*) The sum of 4 or less can occur in four ways: $(3,1), (1,3), (2,1), (1,2)$. Thus $p = \frac{4}{30} = \frac{2}{15}$.

7.22. A class has 12 boys and four girls. Suppose three students are selected at random from the class. Find the probability p that they are all boys.

The probability that the first student selected is a boy is 12/16 since there are 12 boys out of 16 students. If the first student is a boy, then the probability that the second is a boy is 11/15 since there are 11 boys left out of 15 students. Finally, if the first two students selected were boys, then the probability that the third student is a boy is 10/14 since there are 10 boys left out of 14 students. Thus, by the multiplication theorem, the probability that all three are boys is

$$p = \frac{12}{16} \cdot \frac{11}{15} \cdot \frac{10}{14} = \frac{11}{28}$$

Another Method

There are $C(16, 3) = 560$ ways to select three students out of the 16 students, and $C(12, 3) = 220$ ways to select three boys out of 12 boys; hence

$$p = \frac{220}{560} = \frac{11}{28}$$

Another Method

If the students are selected one after the other, then there are $16 \cdot 15 \cdot 14$ ways to select three students,

and $12 \cdot 11 \cdot 10$ ways to select three boys; hence

$$p = \frac{12 \cdot 11 \cdot 10}{16 \cdot 15 \cdot 14} = \frac{11}{28}$$

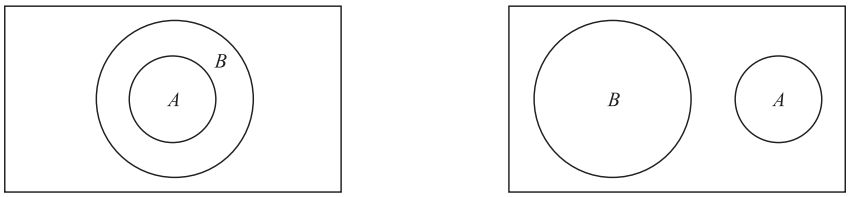
7.23. Find $P(B \mid A)$ if: (*a*) A is a subset of B; (*b*) A and B are mutually exclusive. (Assume $P(A) > 0$.)

(*a*) If A is a subset of B [as pictured in Fig. 7-6(*a*)], then whenever A occurs B must occur; hence $P(B \mid A) = 1$. Alternatively, if A is a subset of B, then $A \cap B = A$; hence

$$P(B \mid A) = \frac{P(A \cap B)}{P(A)} = \frac{P(A)}{P(A)} = 1$$

(*b*) If A and B are mutually exclusive, i.e., disjoint [as pictured in Fig. 7-6(*b*)], then whenever A occurs B cannot occur; hence $P(B \mid A) = 0$. Alternatively, if A and B are disjoint, then $A \cap B = \varnothing$; hence

$$P(B \mid A) = \frac{P(A \cap B)}{P(A)} = \frac{P(= \varnothing)}{P(A)} = \frac{0}{P(A)} = 0$$



(*a*) $A \subseteq B$ (*b*) $A \cap B = \varnothing$

Fig. 7-6

INDEPENDENCE

7.24. The probability that A hits a target is $\frac{1}{3}$ and the probability that B hits a target is $\frac{1}{5}$. They both fire at the target. Find the probability that: (*a*) A does not hit the target, (*b*) both hit the target; (*c*) one of them hits the target; (*d*) neither hits the target.

We are given $P(A) = \frac{1}{3}$ and $P(B) = \frac{1}{5}$ (and we assume the events are independent).

(*a*) P (not A) $= P(A^c) = 1 - P(A) = 1 - \frac{1}{3} = \frac{2}{3}$.

(*b*) Since the events are independent,

$$P(A \text{ and } B) = P(A \cap B) = P(A) \cdot P(B) = \tfrac{1}{3} \cdot \tfrac{1}{5} = \tfrac{1}{15}$$

(*c*) By the Addition Principle (Theorem 7.4),

$$P(A \text{ or } B) = P(A \cup B) = P(A) + P(B) - P(A \cap B) = \tfrac{1}{3} + \tfrac{1}{5} - \tfrac{1}{15} = \tfrac{7}{15}$$

(*d*) We have

$$P(\text{neither } A \text{ nor } B) = P((A \cup B)^c) = 1 - P(A \cup B) = 1 - \tfrac{7}{15} = \tfrac{8}{15}$$

7.25. Consider the following events for a family with children:

$$A = \{\text{children of both sexes}\}, \qquad B = \{\text{at most one boy}\}$$

(*a*) Show that A and B are independent events if a family has three children.

(*b*) Show that A and B are dependent events if a family has only two children.

(*a*) We have the equiprobable space $S = \{bbb, bbg, bgb, bgg, gbb, gbg, ggb, ggg\}$. Here

$$A = \{bbg, bgb, bgg, gbb, gbg, ggb\} \quad \text{and so} \quad P(A) = \tfrac{6}{8} = \tfrac{3}{4}$$
$$B = \{bgg, gbg, ggb, ggg\} \quad \text{and so} \quad P(B) = \tfrac{4}{8} = \tfrac{1}{2}$$
$$A \cap B = \{bgg, gbg, ggb\} \quad \text{and so} \quad P(A \cap B) = \tfrac{3}{8}$$

Since $P(A)P(B) = \frac{3}{4} \cdot \frac{1}{2} = \frac{3}{8} = P(A \cap B)$, A and B are independent.

(*b*) We have the equiprobable space $S = \{bb, bg, gb, gg\}$. Here

$$A = \{bg, gb\} \quad \text{and so} \quad P(A) = \tfrac{1}{2}$$
$$B = \{bg, gb, gg\} \quad \text{and so} \quad P(B) = \tfrac{3}{4}$$
$$A \cap B = \{bg, gb\} \quad \text{and so} \quad P(A \cap B) = \tfrac{1}{2}$$

Since $P(A)P(B) \neq P(A \cap B)$, A and B are dependent.

7.26. Box A contains five red marbles and three blue marbles, and box B contains three red and two blue. A marble is drawn at random from each box.

(*a*) Find the probability p that both marbles are red.

(*b*) Find the probability p that one is red and one is blue.

(*a*) The probability of choosing a red marble from A is $\frac{5}{8}$ and from B is $\frac{3}{5}$. Since the events are independent, $p = \frac{5}{8} \cdot \frac{3}{5} = \frac{3}{8}$.

(*b*) The probability p_1 of choosing a red marble from A and a blue marble from B is $\frac{5}{8} \cdot \frac{2}{5} = \frac{1}{4}$. The probability p_2 of choosing a blue marble from A and a red marble from B is $\frac{3}{8} \cdot \frac{3}{5} = \frac{9}{40}$. Hence $p = p_1 + p_2 = \frac{1}{4} + \frac{9}{40} = \frac{19}{40}$.

7.27. Prove: If A and B are independent events, then A^c and B^c are independent events.

Let $P(A) = x$ and $P(B) = y$. Then $P(A^c) = 1 - x$ and $P(B^c) = 1 - y$. Since A and B are independent. $P(A \cap B) = P(A)P(B) = xy$. Furthermore,

$$P(A \cup B) = P(A) + P(B) - P(A \cap B) = x + y - xy$$

By DeMorgan's law, $(A \cup B)^c = A^c \cap B^c$; hence

$$P(A^c \cap B^c) = P((A \cup B)^c) = 1 - P(A \cup B) = 1 - x - y + xy$$

On the other hand,

$$P(A^c)P(B^c) = (1 - x)(1 - y) = 1 - x - y + xy$$

Thus $P(A^c \cap B^c) = P(A^c)P(B^c)$, and so A^c and B^c are independent.

In similar fashion, we can show that A and B^c, as well as A^c and B, are independent.

REPEATED TRIALS, BINOMIAL DISTRIBUTION

7.28. Whenever horses a, b, c, d race together, their respective probabilities of winning are 0.2, 0.5, 0.1, 0.2. That is, $S = \{a, b, c, d\}$ where $P(a) = 0.2$, $P(b) = 0.5$, $P(c) = 0.1$, and $P(d) = 0.2$. They race three times.

(*a*) Describe and find the number of elements in the product probability space S_3.

(*b*) Find the probability that the same horse wins all three races.

(*c*) Find the probability that a, b, c each win one race.

(*a*) By definition, $S_3 = S \times S \times S = \{(x, y, z)\colon x, y, z \in S\}$ and

$$P((x, y, z) = P(x)P(y)P(z)$$

Thus, in particular, S_3 contains $4^3 = 64$ elements.

(*b*) Writing xyz for (x, y, z), we seek the probability of the event

$$A = \{aaa, bbb, ccc, ddd\}$$

By definition

$$P(aaa) = (0.2)^3 = 0.008, \qquad P(ccc) = (0.1)^3 = 0.001$$
$$P(bbb) = (0.5)^3 = 0.125, \qquad P(ddd) = (0.2)^3 = 0.008$$

Thus $P(A) = 0.0008 + 0.125 + 0.001 + 0.008 = 0.142$.

(*c*) We seek the probability of the event

$$B = \{abc, acb, bac, bca, cab, cba\}$$

Every element in B has the same probability

$(0.2)(0.5)(0.1) = 0.01$. Hence $P(B) = 6(0.01) = 0.06$.

7.29. A fair coin is tossed three times. Find the probability that there will appear: (*a*) three heads; (*b*) exactly two heads; (*c*) exactly one head; (*d*) no heads.

Let H denote a head and T a tail on any toss. The three tosses can be modeled as an equiprobable space in which there are eight possible outcomes:

$$S = \{\text{HHH, HHT, HTH, HTT, THH, THT, TTH, TTT}\}$$

However, since the result on any one toss does not depend on the result of any other toss, the three tosses may be modeled as three independent trials in which $P(H) = \frac{1}{2}$ and $P(T) = \frac{1}{2}$ on any one trial. Then:

(*a*) $P(\text{three heads}) = P(\text{HHH}) = \frac{1}{2} \cdot \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{8}$.

(*b*) $P(\text{exactly two heads}) = P(\text{HHT or HTH or THH})$

$$= \tfrac{1}{2} \cdot \tfrac{1}{2} \cdot \tfrac{1}{2} + \tfrac{1}{2} \cdot \tfrac{1}{2} \cdot \tfrac{1}{2} + \tfrac{1}{2} \cdot \tfrac{1}{2} \cdot \tfrac{1}{2} = \tfrac{3}{8}$$

(*c*) As in (*b*), $P(\text{exactly one head}) = P(\text{exactly two tails}) = \frac{3}{8}$.

(*d*) As in (*a*), $P(\text{no heads}) = P(\text{three tails}) = \frac{1}{8}$.

7.30. The probability that John hits a target is $p = \frac{1}{4}$. He fires $n = 6$ times. Find the probability that he hits the target: (*a*) exactly two times; (*b*) more than four times; (*c*) at least once.

This is a binomial experiment with $n = 6$, $p = \frac{1}{4}$, and $q = 1 - p = \frac{3}{4}$; that is, $B(6, \frac{1}{4})$. Accordingly, we use Theorem 7.7.

(*a*) $P(2) = \binom{6}{2}(\frac{1}{4})^2(\frac{3}{4})^4 = 15(3^4)/(4^6) = \frac{1215}{4096} \approx 0.297$.

(*b*) $P(5) + P(6) = \binom{6}{5}(\frac{1}{4})^5(\frac{3}{4})^1 + (\frac{1}{4})^6 = \frac{18}{4^6} + \frac{1}{4^6} = \frac{19}{4^6} = \frac{19}{4096} \approx 0.0046$.

(*c*) $P(0) = (\frac{3}{4})^6 = \frac{729}{4096}$, so $P(X > 0) = 1 - \frac{729}{4096} = \frac{3367}{4096} \approx 0.82$.

7.31. Suppose 20% of the items produced by a factory are defective. Suppose four items are chosen at random. Find the probability that: (*a*) two are defective; (*b*) three are defective; (*c*) none is defective.

This is a binomial experiment with $n = 4$, $p = 0.2$ and $q = 1 - p = 0.8$; that is, $B(4, 0.2)$. Hence use Theorem 7.7.

(*a*) $P(2) = \binom{4}{2}(0.2)^2(0.8)^2 = 0.1536$.

(*b*) $P(3) = \binom{4}{3}(0.2)^3(0.8)^1 = 0.0256.$

(*c*) $P(0) = (0.8)^4 = 0.4095.$

7.32. Team A has probability $\frac{2}{3}$ of winning whenever it plays. Suppose A plays four games. Find the probability p that A wins more than half of its games.

Here $n = 4$, $p = \frac{2}{3}$ and $q = 1 - p = \frac{1}{3}$. A wins more than half its games if it wins three or four games. Hence

$$p = P(3) + P(4) = \binom{4}{3}\left(\frac{2}{3}\right)^3\left(\frac{1}{3}\right)^1 + \binom{4}{4}\left(\frac{2}{3}\right)^4 = \frac{32}{81} + \frac{16}{81} = \frac{16}{27} = 0.59$$

7.33. A family has six children. Find the probability p that there are: (*a*) three boys and three girls; (*b*) fewer boys than girls. Assume that the probability of any particular child being a boy is $\frac{1}{2}$.

Here $n = 6$ and $p = q = \frac{1}{2}$.

(*a*) $p = P(3 \text{ boys}) = \binom{6}{3}\left(\frac{1}{2}\right)^3\left(\frac{1}{2}\right)^2 = \frac{20}{64} = \frac{5}{16}.$

(*b*) There are fewer boys than girls if there are zero, one, or two boys. Hence

$$p = P(0 \text{ boys}) + P(1 \text{ boy}) + P(2 \text{ boys}) = \left(\frac{1}{2}\right)^6 + \binom{6}{1}\left(\frac{1}{2}\right)^5 + \binom{6}{2}\left(\frac{1}{2}\right)^2\left(\frac{1}{2}\right)^4 = \frac{11}{32} = 0.34$$

7.34. A certain type of missile hits its target with probability $p = 0.3$. Find the number of missiles that should be fired so that there is at least an 80% probability of hitting the target.

The probability of missing the target is $q = 1 - p = 0.7$. Hence the probability that n missiles miss the target is $(0.7)^n$. Thus we seek the smallest n for which

$$1 - (0.7)^n > 0.8 \qquad \text{or equivalently} \qquad (0.7)^n < 0.2$$

Compute:

$$(0.7)^1 = 0.7, \qquad (0.7)^2 = 0.49, \qquad (0.7)^3 = 0.343, \qquad (0.7)^4 = 0.2401, \qquad (0.7)^5 = 0.16807$$

Thus at least five missiles should be fired.

7.35. How many dice should be thrown so that there is a better than an even chance of obtaining a six?

The probability of not obtaining a six on n dice is $\left(\frac{5}{6}\right)^n$. Hence we seek the smallest n for which $\left(\frac{5}{6}\right)^n$ is less than $\frac{1}{2}$. Compute as follows:

$$\left(\frac{5}{6}\right)^1 = \frac{5}{6}, \qquad \left(\frac{5}{6}\right)^2 = \frac{25}{36}, \qquad \left(\frac{5}{6}\right)^3 = \frac{125}{216}, \qquad \text{but} \qquad \left(\frac{5}{6}\right)^4 = \frac{625}{1296} < \frac{1}{2}$$

Thus four dice must be thrown.

7.36. A certain soccer team wins (W) with probability 0.6, losses (L) with probability 0.3, and ties (T) with probability 0.1. The team plays three games over the weekend. (*a*) Determine the elements of the event A that the team wins at least twice and does not lose; and find $P(A)$. (*b*) Determine the elements of the event B that the team wins, loses, and ties in some order; and find $P(B)$.

(*a*) A consists of all ordered triples with at least two Ws and no Ls. Thus

$$A = \{\text{WWW, WWT, WTW, TWW}\}$$

Furthermore,

$$\begin{aligned} P(A) &= P(\text{WWW}) + P(\text{WWT}) + P(\text{WTW}) + P(\text{TWW}) \\ &= (0.6)(0.6)(0.6) + (0.6)(0.6)(0.1) + (0.6)(0.1)(0.6) + (0.1)(0.6)(0.6) \\ &= 0.216 + 0.036 + 0.036 + 0.036 = 0.324 \end{aligned}$$

(*b*) Here $B = \{\text{WLT, WTL, LWT, LTW, TWL, TLW}\}$. Every element in B has probability $(0.6)(0.3)(0.1) = 0.018$; hence $P(B) = 6(0.018) = 0.108$.

7.37. A man fires at a target $n = 6$ times and hits it $k = 2$ times. (*a*) List the different ways that this can happen. (*b*) How many ways are there?

(*a*) List all sequences with two Ss (successes) and four Fs (failures):

SSFFFF, SFSFFF, SFFSFF, SFFFSF, SFFFFS, FSSFFF, FSFSFF, FSFFSF, FSFFFS, FFSSFF, FFSFSF, FFSFFS, FFFSSF, FFFSFS, FFFFSS

(*b*) There are 15 different ways as indicated by the list. Observe that this is equal to $\binom{6}{2}$ since we are distributing $k = 2$ letters S among the $n = 6$ positions in the sequence.

7.38. Prove Theorem 7.7: The probability of exactly k successes in a binomial experiment $B(n, p)$ is given by

$$P(k) = P(k \text{ successes}) = \binom{n}{k} p^k q^{n-k}$$

The probability of one or more successes is $1 - q^n$.

The sample space of the n repeated trials consists of all n-tuples (i.e., n-element sequences) whose components are either S (success) or F (failure). Let A be the event of exactly k successes. Then A consists of all n-tuples of which k components are S and $n - k$ components are F. The number of such n-tuples in the event A is equal to the number of ways that k letters S can be distributed among the n components of an n-tuple; hence A consists of $C(n,k) = \binom{n}{k}$ sample points. The probability of each point in A is $p^k q^{n-k}$; hence

$$P(A) = \binom{n}{k} p^k q^{n-k}$$

In particular, the probability of no successes is

$$P(0) = \binom{n}{0} p^0 q^n = q^n$$

Thus the probability of one or more successes is $1 - q^n$.

RANDOM VARIABLES, EXPECTATION

7.39. A player tosses two fair coins. He wins \$2 if two heads occur, and \$1 if one head occurs. On the other hand, he loses \$3 if no heads occur. Find the expected value E of the game. Is the game fair? (The game is fair, favorable, or unfavorable to the player according as $E = 0$, $E > 0$ or $E < 0$.]

The sample space is $S = \{\text{HH, HT, TH, TT}\}$ and each sample point has probability $\frac{1}{4}$. For the player's gain, we have

$$X(\text{HH}) = \$2, \qquad X(\text{HT}) = X(\text{TH}) = \$1, \qquad X(\text{TT}) = -\$3$$

and so the distribution of X is

x_i	2	1	−3
p_i	$\frac{1}{4}$	$\frac{2}{4}$	$\frac{1}{4}$

and $$E = E(X) = 2\left(\tfrac{1}{4}\right) + 1\left(\tfrac{2}{4}\right) - 3\left(\tfrac{1}{4}\right) = \$0.25$$

Since $E(X) > 0$, the game is favourable to the player.

7.40. Two numbers from 1 to 3 are chosen at random with repetitions allowed. Let X denote the sum of the numbers. (*a*) Find the distribution of X. (*b*) Find the expectation $E(X)$.

(*a*) There are nine equiprobable pairs making up the sample space S. X assumes the values 2, 3, 4, 5, 6 with the following probabilities:

$$P(2) = P(1,1) = \tfrac{1}{9}, \qquad P(3) = P(\{(1,2),(2,1)\}) = \tfrac{2}{9}$$
$$P(4) = P(\{(1,3),(2,2),(3,1)\}) = \tfrac{3}{9}$$
$$P(5) = P(\{(2,3),(3,2)\}) = \tfrac{2}{9}, \qquad P(6) = P(3,3) = \tfrac{1}{9}$$

Hence, the distribution is

x_i	2	3	4	5	6
$P(x_i)$	$\frac{1}{9}$	$\frac{2}{9}$	$\frac{3}{9}$	$\frac{2}{9}$	$\frac{1}{9}$

(*b*) The expected value $E(X)$ is obtained by multiplying each value of x by its probability and taking the sum. Hence

$$E(X) = 2\left(\tfrac{1}{9}\right) + 3\left(\tfrac{2}{9}\right) + 4\left(\tfrac{3}{9}\right) + 5\left(\tfrac{2}{9}\right) + 6\left(\tfrac{1}{9}\right) = \tfrac{36}{9} = 4$$

7.41. A coin is weighted so that $P(H) = \frac{3}{4}$ and $P(T) = \frac{1}{4}$. The coin is tossed three times. Let X denote the number of heads that appear. (*a*) Find the distribution of X. (*b*) Find the expectation $E(X)$.

(*a*) The sample space is

$$S = \{\text{HHH, HHT, HTH, HTT, THH, THT, TTH, TTT}\}$$

X assumes the values 0, 1, 2, 3 with the following probabilities:

$$P(0) = P(\text{TTT} = \tfrac{1}{4}\cdot\tfrac{1}{4}\cdot\tfrac{1}{4} = \tfrac{1}{64}$$
$$P(1) = P(\text{HTT, THT, TTH}) = \tfrac{3}{4}\cdot\tfrac{1}{4}\cdot\tfrac{1}{4} + \tfrac{1}{4}\cdot\tfrac{3}{4}\cdot\tfrac{1}{4} + \tfrac{1}{4}\cdot\tfrac{1}{4}\cdot\tfrac{3}{4} = \tfrac{9}{64}$$
$$P(2) = P(\text{HHT, HTH, THH}) = \tfrac{3}{4}\cdot\tfrac{3}{4}\cdot\tfrac{1}{4} + \tfrac{3}{4}\cdot\tfrac{1}{4}\cdot\tfrac{3}{4} + \tfrac{1}{4}\cdot\tfrac{3}{4}\cdot\tfrac{3}{4} = \tfrac{27}{64}$$
$$P(3) = P(\text{HHH}) = \tfrac{3}{4}\cdot\tfrac{3}{4}\cdot\tfrac{3}{4} = \tfrac{27}{64}$$

Hence, the distribution is as follows:

x_i	0	1	2	3
$P(x_i)$	$\frac{1}{64}$	$\frac{9}{64}$	$\frac{27}{64}$	$\frac{27}{64}$

(*b*) The expected value $E(X)$ is obtained by multiplying each value of x by its probability and taking the sum. Hence

$$E(X) = 0\left(\tfrac{1}{64}\right) + 1\left(\tfrac{9}{64}\right) + 2\left(\tfrac{27}{64}\right) + 3\left(\tfrac{27}{64}\right) = \tfrac{144}{64} = 2.25$$

7.42. You have won a contest. Your prize is to select one of three envelopes and keep what is in it. Each of two of the envelopes contains a check for \$30, but the third envelope contains a check for \$3000. What is the expectation E of your winnings (as a probability distribution)?

Let X denote your winnings. Then $X = 30$ or 3000, and $P(30) = \frac{2}{3}$ and $P(3000) = \frac{1}{3}$. Hence

$$E = E(X) = 30\cdot\tfrac{2}{3} + 3000\cdot\tfrac{1}{3} = 20 + 1000 = 1020$$

7.43. A fair coin is tossed until a head or five tails occurs. Find the expected number E of tosses of the coin.

The possible outcomes are

$$\text{H}, \quad \text{TH}, \quad \text{TTH}, \quad \text{TTTH}, \quad \text{TTTTH}, \quad \text{TTTTT}$$

with respective probabilities (independent trials)

$$\tfrac{1}{2}, \quad \left(\tfrac{1}{2}\right)^2 = \tfrac{1}{4}, \quad \left(\tfrac{1}{2}\right)^3 = \tfrac{1}{8}, \quad \left(\tfrac{1}{2}\right)^4 = \tfrac{1}{16}, \quad \left(\tfrac{1}{2}\right)^5 = \tfrac{1}{32}, \quad \left(\tfrac{1}{2}\right)^5 = \tfrac{1}{32}$$

The random variable X of interest is the number of tosses in each outcome. Thus

$$X(\text{H}) = 1, \quad X(\text{TTH}) = 3, \quad X(\text{TTTTH}) = 5$$
$$X(\text{TH}) = 2, \quad X(\text{TTTH}) = 4, \quad X(\text{TTTTT}) = 5$$

and these X values are assigned the probabilities

$$P(1) = P(\text{H}) = \tfrac{1}{2}, \quad P(3) = P(\text{TTH}) = \tfrac{1}{8}, \quad P(5) = P(\text{TTTTH}) + P(\text{TTTTT})$$
$$P(2) = P(\text{TH}) = \tfrac{1}{4}, \quad P(4) = P(\text{TTTH}) = \tfrac{1}{16}, \quad = \tfrac{1}{32} + \tfrac{1}{32} = \tfrac{1}{16}$$

Accordingly,

$$E = E(X) = 1 \cdot \tfrac{1}{2} + 2 \cdot \tfrac{1}{4} + 3 \cdot \tfrac{1}{8} + 4 \cdot \tfrac{1}{16} + 5 \cdot \tfrac{1}{16} \approx 1.9$$

7.44. A linear array EMPLOYEE has n elements. Suppose NAME appears randomly in the array, and there is a linear search to find the location K of NAME, that is, to find K such that EMPLOYEE[K] = NAME. Let $f(n)$ denote the number of comparisons in the linear search.

(*a*) Find the expected value of $f(n)$.

(*b*) Find the maximum value (worst case) of $f(n)$.

(*a*) Let X denote the number of comparisons. Since NAME can appear in any position in the array with the same probability of $1/n$, we have $X = 1, 2, 3, \ldots, n$, each with probability $1/n$. Hence

$$f(n) = E(X) = 1 \cdot \frac{1}{n} + 2 \cdot \frac{1}{n} + 3 \cdot \frac{1}{n} + \cdots + n \cdot \frac{1}{n}$$
$$= (1 + 2 + \cdots + n) \cdot \frac{1}{n} = \frac{n(n+1)}{2} \cdot \frac{1}{n} = \frac{n+1}{2}$$

(*b*) If NAME appears at the end of the array, then $f(n) = n$.

MEAN, VARIANCE, AND STANDARD DEVIATION

7.45. Find the mean $\mu = E(X)$, variance $\sigma^2 = \text{Var}(X)$, and standard deviation $\sigma = \sigma_X$ of each distribution:

(*a*)

x_i	2	3	11
p_i	$\frac{1}{3}$	$\frac{1}{2}$	$\frac{1}{6}$

(*b*)

x_i	1	3	4	5
p_i	0.4	0.1	0.2	0.3

Use the formulas,

$$\mu = E(X) = x_1p_1 + x_2p_2 + \cdots + x_mp_m = \Sigma x_ip_i, \qquad \sigma^2 = \text{Var}(X) = E(X^2) - \mu^2$$
$$E(X^2) = x_1^2p_1 + x_2^2p_2 + \cdots + x_m^2p_m = \Sigma x_i^2p_i, \qquad \sigma = \sigma_X = \sqrt{\text{Var}(X)}$$
$$\sigma = \sigma_X = \sqrt{\text{Var}(X)}$$

(*a*) $\mu = \Sigma x_ip_i = 2\left(\tfrac{1}{3}\right) + 3\left(\tfrac{1}{2}\right) + 11\left(\tfrac{1}{6}\right) = 4.$

$E(X^2) = \Sigma x_i^2p_i = 2^2\left(\tfrac{1}{3}\right) + 3^2\left(\tfrac{1}{2}\right) + 11^2\left(\tfrac{1}{6}\right) = 26.$

$\sigma^2 = \text{Var}(X) = E(X^2) - \mu^2 = 26 - 4^2 = 10.$

$\sigma = \sqrt{\text{Var}(X)} = \sqrt{10} = 3.2.$

(*b*) $\mu = \Sigma x_i p_i = 1(0.4) + 3(0.1) + 4(0.2) + 5(0.3) = 3.$
$E(X^2) = \Sigma x_i^2 p_i = 1(0.4) + 9(0.1) + 16(0.2) + 25(0.3) = 12.$
$\sigma^2 = \text{Var}\,(X) = E(X^2) - \mu^2 = 12 - 9 = 3.$
$\sigma = \sqrt{\text{Var}\,(X)} = \sqrt{3} = 1.7.$

7.46. Five cards are numbered 1 to 5. Two cards are drawn at random. Let X denote the sum of the numbers drawn.

(*a*) Find the distribution of X.

(*b*) Find the mean μ, variance $\sigma^2 = \text{Var}\,(X)$, and standard deviation $\sigma = \sigma_X$ of X.

(*a*) There are $C(5,2) = 10$ ways of drawing two cards at random. The 10 equiprobable sample points, with their corresponding X values, are shown below:

$$\{1,2\} \to 3 \quad \{1,3\} \to 4 \quad \{1,4\} \to 5 \quad \{1,5\} \to 6 \quad \{2,3\} \to 5$$
$$\{2,4\} \to 6 \quad \{2,5\} \to 7 \quad \{3,4\} \to 7 \quad \{3,5\} \to 8 \quad \{4,5\} \to 9$$

Observe that the values of X are the seven numbers 3, 4, 5, 6, 7, 8, and 9; of these 3, 4, 8, and 9 are each assumed at one sample point, while 5, 6, and 7 are each assumed at two sample points. Hence the distribution of X is

x_i	3	4	5	6	7	8	9
p_i	0.1	0.1	0.2	0.2	0.2	0.1	0.1

(*b*) $\mu = E(X) = \Sigma x_i p_i = 3(0.1) + 4(0.1) + 5(0.2) + 6(0.2) + 7(0.2) + 8(0.1) + 9(0.1) = 6.$
$E(X^2) - \Sigma x_i^2 p_i = 9(0.1) + 16(0.1) + 25(0.2) + 36(0.2) + 49(0.2) + 64(0.1) + 81(0.1) = 39.$
$\text{Var}\,(X) = E(X^2) - \mu^2 = 39 - 6^2 = 3.$
$\sigma = \sqrt{\text{Var}\,(X)} = \sqrt{3} \approx 1.7.$

7.47. A pair of fair dice is thrown. Let X denote the maximum of the two numbers which appear.

(*a*) Find the distribution of X.

(*b*) Find the mean μ, variance $\sigma^2 = \text{Var}\,(X)$, and standard deviation $\sigma = \sigma_X$ of X.

(*a*) The sample space S is the equiprobable space consisting of the 36 pairs of integers (a, b) where a and b range from 1 to 6; that is,

$$S = \{(1,1), (1,2), \ldots, (6,6)\}$$

(See Problem 7.3.) Since X assigns to each pair in S the larger of the two integers, the values of X are the integers from 1 to 6. Observe:

(i) Only one pair $(1,1)$ give a maximum of 1; hence $P(1) = \frac{1}{36}$.

(ii) Three pairs, $(1,2), (2,2), (2,1)$, give a maximum of 2; hence $P(2) = \frac{3}{36}$.

(iii) Five pairs, $(1,3), (2,3), (3,3), (3,2), (3,1)$, give a maximum of 3; hence $P(3) = \frac{5}{36}$.

Similarly, $P(4) = \frac{7}{36}$, $P(5) = \frac{9}{36}$, $P(6) = \frac{11}{36}$.

Thus the distribution of X is as follows:

x_i	1	2	3	4	5	6
p_i	$\frac{1}{36}$	$\frac{3}{36}$	$\frac{5}{36}$	$\frac{7}{36}$	$\frac{9}{36}$	$\frac{11}{36}$

(*b*) We find the expectation (mean) of X by multiplying each x_i by its probability p_i and then summing:

$$\mu = E(X) = 1 \cdot \tfrac{1}{36} + 2 \cdot \tfrac{3}{36} + 3 \cdot \tfrac{5}{36} + 4 \cdot \tfrac{7}{36} + 5 \cdot \tfrac{9}{36} + 6 \cdot \tfrac{11}{36} = \tfrac{161}{36} \approx 4.5$$

We find $E(X^2)$ by multiplying x_i^2 by p_i and taking the sum:

$$E(X^2) = 1 \cdot \tfrac{1}{36} + 4 \cdot \tfrac{3}{36} + 9 \cdot \tfrac{5}{36} + 16 \cdot \tfrac{7}{36} + 25 \cdot \tfrac{9}{36} + 36 \cdot \tfrac{11}{36} = \tfrac{791}{36} \approx 22.0$$

Then

$$\mathrm{Var}(X) = E(X^2) - \mu^2 = 22.0 - (4.5)^2 = 1.75 \qquad \text{and} \qquad \sigma_x = \sqrt{1.75} \approx 1.3$$

7.48. A fair die is tossed. Let X denote twice the number appearing, and let Y be 1 or 3 according as an odd or even number appears. Find the distribution and expectation: (*a*) of X; (*b*) of Y.

The sample space is $S = \{1, 2, 3, 4, 5, 6\}$, with each sample point having probability $\frac{1}{6}$.

(*a*) The images of the sample points are:

$$X(1) = 2, \qquad X(2) = 4, \qquad X(3) = 6, \qquad X(4) = 8, \qquad X(5) = 10, \qquad X(6) = 12$$

As these are distinct, the distribution of X is

x_i	2	4	6	8	10	12
$P(x_i)$	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{6}$

Thus

$$E(X) = \sum x_i P(x_i) = \tfrac{2}{6} + \tfrac{4}{6} + \tfrac{6}{6} + \tfrac{8}{6} + \tfrac{10}{6} + \tfrac{12}{6} = 7$$

(*b*) The images of the sample points are:

$$Y(1) = 1, \qquad Y(2) = 3, \qquad Y(3) = 1, \qquad Y(4) = 3, \qquad Y(5) = 1, \qquad Y(6) = 3$$

The two Y-values, 1 and 3, are each assumed at three sample points. Hence we have the distribution

y_i	1	3
$P(y_i)$	$\frac{3}{6}$	$\frac{3}{6}$

Thus

$$E(Y) = \sum y_i P(y_i) = \tfrac{3}{6} + \tfrac{9}{6} = 2$$

7.49. Let X and Y be random variables defined on the same sample space S. Then $Z = X + Y$ and $W = XY$ are also random variables on S defined by

$$Z(s) = (X + Y)(s) = X(s) + Y(s) \qquad \text{and} \qquad W(s) = (XY)(s) = X(s)Y(s)$$

Let X and Y be the random variable in Problem 7.48.

(*a*) Find the distribution and expectation of $Z = X + Y$.
Verify that $E(X + Y) = E(X) + E(Y)$.

(*b*) Find the distribution and expectation of $W = XY$.

The sample space is still $S = \{1, 2, 3, 4, 5, 6\}$, and each sample point still has probability $\frac{1}{6}$.

(*a*) Using $(X + Y)(s) = X(s) + Y(s)$ and the values of X and Y from Problems 7.48, we obtain:

$$(X + Y)(1) = 2 + 1 = 3, \qquad (X + Y)(3) = 6 + 1 = 7, \qquad (X + Y)(5) = 10 + 1 = 11$$
$$(X + Y)(2) = 4 + 3 = 7, \qquad (X + Y)(4) = 8 + 3 = 11, \qquad (X + Y)(6) = 12 + 3 = 15$$

The image set is $\{3, 7, 11, 5\}$. The values 3 and 15 are each assumed at only one sample point and hence have probability $\frac{1}{6}$; the values 7 and 11 are each assumed at two sample points and hence have probability $\frac{2}{6}$. Thus the distribution of $Z = X + Y$ is:

z_i	3	7	11	15
$P(z_i)$	1/6	2/6	2/6	1/6

Thus

$$E(X + Y) = E(Z) = \sum z_i P(z_i) = \tfrac{3}{6} + \tfrac{14}{6} + \tfrac{22}{6} + \tfrac{15}{6} = 9$$

Moreover,

$$E(X + Y) = 9 = 7 + 2 = E(X) + E(Y)$$

(*b*) Using $(XY)(s) = X(s)Y(s)$, we obtain:

$$(XY)(1) = 2(1) = 2, \qquad (XY)(3) = 6(1) = 6, \qquad (XY)(5) = 10(1) = 10$$
$$(XY)(2) = 4(3) = 12, \qquad (XY)(4) = 8(3) = 24, \qquad (XY)(6) = 12(3) = 36$$

Each value of XY is assumed at just one sample point; hence the distribution of $W = XY$ is:

w_i	2	6	10	12	24	36
$P(w_i)$	1/6	1/6	1/6	1/6	1/6	1/6

Thus

$$E(XY) = E(W) = \sum w_i P(w_i) = \tfrac{2}{6} + \tfrac{6}{6} + \tfrac{10}{6} + \tfrac{12}{6} + \tfrac{24}{6} + \tfrac{36}{6} = 15$$

[Note $E(XY) = 15 \neq (7)(2) = E(X)E(Y)$.]

7.50. The probability that a man hits a target is $p = 0.1$. He fires $n = 100$ times. Find the expected number μ of times he will hit the target, and the standard deviation σ.

This is a binomial experiment $B(n, p)$ where $n = 100$, $p = 0.1$, and $q = 1 - p = 0.9$. Accordingly, we apply Theorem 7.9 to obtain

$$\mu = np = 100(0.1) = 10 \qquad \text{and} \qquad \sigma = \sqrt{npq} = \sqrt{100(0.1)(0.9)} = 3$$

7.51. A student takes an 18-question multiple-choice exam, with four choices per question. Suppose one of the choices is obviously incorrect, and the student makes an "educated" guess of the remaining choices. Find the expected number $E(X)$ of correct answers, and the standard deviation σ.

This is a binomial experiment $B(n, p)$ where $n = 18$, $p = \frac{1}{3}$, and $q = 1 - p = \frac{2}{3}$. Hence

$$E(X) = np = 18 \cdot \frac{1}{3} = 6 \qquad \text{and} \qquad \sigma = \sqrt{npq} = \sqrt{18 \cdot \frac{1}{3} \cdot \frac{2}{3}} = 2$$

7.52. The expectation function $E(X)$ on the space of random variables on a sample space S can be proved to be *linear*, that is,

$$E(X_1 + X_2 + \cdots + x_n) = E(X_1) + E(X_2) + \cdots + E(X_n)$$

Use this property to prove $\mu = np$ for a binomial experiment $B(n, p)$.

On the sample space of n Bernoulli trials, let X_i (for $i = 1, 2, \ldots, n$) be the random variable which has the value 1 or 0 according as the ith trial is a success or a failure. Then each X_i has the distribution

x	0	1
$P(x)$	q	p

Thus $E(X_i) = 0(q) + 1(p) = p$. The total number of successes in n trials is

$$X = X_1 + X_2 + \cdots + X_n$$

Using the linearity property of E, we have

$$\begin{aligned} E(X) &= E(X_1 + X_2 + \cdots + X_n) \\ &= E(X_1) + E(X_2) + \cdots + E(X_n) \\ &= p + p + \cdots + p = np \end{aligned}$$

Supplementary Problems

SAMPLE SPACES AND EVENTS

7.53. Let A and B be events. Rewrite each of the following events using set notation: (a) A or not B occurs; (b) only A occurs.

7.54. Let A, B, and C be events. Rewrite each of the following events using set notation: (a) A and B but not C occurs; (b) A or C, but not B occurs; (c) none of the events occurs; (d) at least two of the events occur.

7.55. A penny, a dime, and a die are tossed.

(a) Describe a suitable sample space S, and find $n(S)$.

(b) Express explicitly the following events:

$$A = \{\text{two heads and an even number}\}, \qquad B = \{2 \text{ appears}\}$$

$$C = \{\text{exactly one heads and an odd number}\}$$

(c) Express explicitly the events: (i) A and B; (ii) only B; (iii) B and C.

FINITE EQUIPROBABLE SPACES

7.56. Determine the probability of each event:

(a) An odd number appears in the toss of a fair die.

(b) One or more heads appear in the toss of four fair coins.

(c) One or both numbers exceed 4 in the toss of two fair dice.

7.57. A student is chosen at random to represent a class with five freshman, eight sophomores, three juniors, and two seniors. Find the probability that the student is: (a) a sophomore; (b) a junior; (c) a junior or a senior.

7.58. One card is selected at random from 50 cards numbered 1 to 50. Find the probability that the number on the card is: (*a*) greater than 10; (*b*) divisible by 5; (*c*) greater than 10 and divisible by 5; (*d*) greater than 10 or divisible by 5.

7.59. Of 10 girls in a class, three have blue eyes. Two of the girls are chosen at random. Find the probability that: (*a*) both have blue eyes; (*b*) neither has blue eyes; (*c*) at least one has blue eyes; (*d*) exactly one has blue eyes.

7.60. Ten students, A, B, ..., are in a class. A committee of three is chosen at random to represent the class. Find the probability that: (*a*) A belongs to the committee; (*b*) B belongs to the committee; (*c*) A and B belong to the committee; (*d*) A or B belong to the committee.

7.61. Three bolts and three nuts are in a box. Two parts are chosen at random. Find the probability that one is a bolt and one is a nut.

7.62. A box contains two white socks, two blue socks, and two red socks. Two socks are drawn at random. Find the probability they are a match (same color).

7.63. Of 120 students, 60 are studying French, 50 are studying Spanish, and 20 are studying both French and Spanish. A student is chosen at random. Find the probability that the student is studying: (*a*) French or Spanish; (*b*) neither French nor Spanish; (*c*) only French; (*d*) exactly one of the two languages.

7.64. Three boys and three girls sit randomly in a row. Find the probability that: (*a*) the three girls sit together; (*b*) the boys and girls sit in alternate seats.

FINITE PROBABILITY SPACES

7.65. Under which of the following functions does $S = \{a_1, a_2, a_3\}$ become a probability space?

(*a*) $P(a_1) = \frac{1}{4}, P(a_2) = \frac{1}{3}, P(a_3) = \frac{1}{2}$.
(*b*) $P(a_1) = \frac{2}{3}, P(a_2) = -\frac{1}{3}, P(a_3) = \frac{2}{3}$.
(*c*) $P(a_1) = \frac{1}{6}, P(a_2) = \frac{1}{3}, P(a_3) = \frac{1}{2}$.
(*d*) $P(a_1) = 0, P(a_2) = \frac{1}{3}, P(a_3) = \frac{2}{3}$.

7.66. A coin is weighted so that heads is three times as likely to appear as tails. Find $P(H)$ and $P(T)$.

7.67. Three students A, B, and C are in a swimming race. A and B have the same probability of winning and each is twice as likely to win as C. Find the probability that: (*a*) B wins; (*b*) C wins; (*c*) B or C wins.

7.68. Consider the following probability distribution:

Outcome	1	2	3	4	5	6
Probability	0.1	0.4	0.1	0.1	0.2	0.1

Find the following probabilities where:

$$A = \{\text{even number}\}, \qquad B = \{2, 3, 4, 5\}, \qquad C = \{1, 2\}$$

(*a*) $P(A)$, $P(B)$, $P(C)$; (*b*) $P(A \cap B)$, $P(A \cup C)$, $P(B \cap C)$.

7.69. Suppose A and B are events with $P(A) = 0.7$, $P(B) = 0.5$, and $P(A \cap B) = 0.4$. Find the probability that: (*a*) A does not occur; (*b*) A or B occurs; (*c*) A but not B occurs; (*d*) neither A nor B occurs.

7.70. Suppose A and B are events with $P(A) = 0.6$, $P(B^c) = 0.3$, and $P(A \cup B) = 0.8$. Find:

(*a*) $P(A \cap B)$; (*b*) $P(A \cap B^c)$; (*c*) $P(A^c \cap B^c)$; (*d*) $P(A^c \cup B^c)$.

CONDITIONAL PROBABILITY, INDEPENDENCE

7.71. A fair die is tossed. Consider events $A = \{2, 4, 6\}$, $B = \{1, 2\}$, $C = \{1, 2, 3, 4\}$. Find:

(*a*) $P(A \text{ and } B)$ and $P(A \text{ or } C)$,

(*b*) $P(A \mid B)$ and $P(B \mid A)$,

(*c*) $P(A \mid C)$ and $P(C \mid A)$.

(*d*) $P(B \mid C)$ and $P(C \mid B)$.

(*e*) Are A and B independent? A and C? B and C?

7.72. A pair of fair dice is tossed. If the numbers appearing are different, find the probability that: (*a*) the sum is even, (*b*) the sum exceeds nine.

7.73. Let A and B be events with $P(A) = 0.6$, $P(B) = 0.3$, and $P(A \cap B) = 0.2$. Find:

(*a*) $P(A \cup B)$; (*b*) $P(A \mid B)$, (*c*) $P(B \mid A)$.

7.74. Let A and B be events with $P(A) = \frac{1}{3}$, $P(B) = \frac{1}{4}$, and $P(A \cup B) = \frac{1}{2}$.

(*a*) Find $P(A \mid B)$ and $P(B \mid A)$.

(*b*) Are A and B independent?

7.75. Let A and B be events with $P(A) = 0.3$, $P(A \cup B) = 0.5$, and $P(B) = p$. Find p if:

(*a*) A and B are mutually disjoint: (*b*) A and B are independent; (*c*) A is a subset of B.

7.76. Let A and B be independent events with $P(A) = 0.3$ and $P(B) = 0.4$. Find:

(*a*) $P(A \cap B)$ and $P(A \cup B)$; (*b*) $P(A \mid B)$ and $P(B \mid A)$.

7.77. In a country club, 60% of the members play tennis, 40% play golf, and 20% play both tennis and golf. A member is chosen at random.

(*a*) Find the probability she plays neither tennis nor golf.

(*b*) If she plays tennis, find the probability she plays golf.

(*c*) If she plays golf, find the probability she plays tennis.

7.78. Box A contains six red marbles and two blue marbles, and box B contains two red and four blue. A marble is drawn at random from each box.

(*a*) Find the probability p that both marbles are red.

(*b*) Find the probability p that one is red and one is blue.

7.79. The probability that A hits a target is $\frac{1}{4}$ and the probability that B hits a target is $\frac{1}{3}$.

(*a*) If each fires twice, what is the probability that the target will be hit at least once?

(*b*) If each fires once and the target is hit only once, what is the probability that A hit the target?

7.80. Three fair coins are tossed. Consider the events:

$$A = \{\text{all heads or all tails}\}, \qquad B = \{\text{at least two heads}\}, \qquad C = \{\text{at most two heads}\}$$

Of the pairs (A, B), (A, C), and (B, C), which are independent? Which are dependent?

REPEATED TRIALS, BINOMIAL DISTRIBUTION

7.81. Whenever horses a, b, and c race together, their respective probabilities of winning are 0.3, 0.5, and 0.2. They race three times.

(a) Find the probability that the same horse wins all three races.

(b) Find the probability that a, b, c each win one race.

7.82. The batting average of a baseball player is 0.300. He comes to bat four times. Find the probability that he will get: (a) exactly two hits; (b) at least one hit.

7.83. The probability that Tom scores on a three-point basketball shot is $p = 0.4$. He shoots $n = 5$ times. Find the probability that he scores: (a) exactly two times; (b) at least once.

7.84. A team wins (W) with probability 0.5, loses (L) with probability 0.3, and ties (T) with probability 0.2. The team plays twice. (a) Determine the sample space S and the probability of each elementary event. (b) Find the probability that the team wins at least once.

7.85. A certain type of missile hits its target with probability $p = \frac{1}{3}$. (a) If three missiles are fired, find the probability that the target is hit at least once. (b) Find the number of missiles that should be fired so that there is at least a 90% probability of hitting the target.

RANDOM VARIABLES

7.86. A pair of dice is thrown. Let X denote the minimum of the two numbers which occur. Find the distributions and expectation of X.

7.87. A fair coin is tossed four times. Let X denote the longest string of heads. Find the distribution and expectation of X.

7.88. A coin, weighted so that $P(H) = \frac{1}{3}$ and $P(T) = \frac{1}{2}$, is tossed until a head or five tails occur. Find the expected number of tosses of the coin.

7.89. The probability of team A winning any game is $\frac{1}{2}$. Suppose A plays B in a tournament. The first team to win two games in a row or three games wins the tournament. Find the expected number of games in the tournament.

7.90. A box contains 10 transistors of which two are defective. A transistor is selected from the box and tested until a nondefective one is chosen. Find the expected number of transistors to be chosen.

7.91. A lottery with 500 tickets gives one prize of \$100, three prizes of \$50 each, and five prizes of \$25 each. (a) Find the expected winnings of a ticket. (b) If a ticket costs \$1, what is the expected value of the game?

7.92. A player tosses three fair coins. He wins \$5 if three heads occur, \$3 if two heads occur, and \$1 if only one head occurs. On the other hand, he loses \$15 if three tails occur. Find the value of the game to the player.

MEAN, VARIANCE, AND STANDARD DEVIATION

7.93. Find the mean μ, variance σ^2, and standard deviation σ of each distribution:

(a)

x_i	2	3	8
p_i	$\frac{1}{4}$	$\frac{1}{2}$	$\frac{1}{4}$

(b)

x_i	-1	0	1	2	3
p_i	0.3	0.1	0.1	0.3	0.2

7.94. Find the mean μ, variance σ^2, and standard deviation σ of following two-point distribution where $p + q = 1$:

x_i	a	b
$f(x_i)$	p	q

7.95. Two cards are selected from a box which contains five cards numbered 1, 1, 2, 2, and 3. Let X denote the sum and Y the maximum of the two numbers drawn. Find the distribution, mean, variance, and standard deviation of the random variables: (*a*) X; (*b*) Y; (*c*) $Z = X + Y$; (*d*) $W = XY$. (See Problem 7.49 for the definitions of $Z = X + Y$ and $W = XY$.)

7.96. Team A has probability $p = 0.8$ of winning each time it plays. Let X denote the number of times A will win in $n = 100$ games. Find the mean μ, variance σ^2, and standard deviation σ of X.

7.97. An unprepared student takes a five-question true-false quiz and guesses every answer. Find the probability that the student will pass the quiz if at least four correct answers is the passing grade.

7.98. Let X be a binomially distributed random variable $B(n, p)$ with $E(X) = 2$ and $\text{Var}(X) = \frac{4}{3}$. Find n and p.

Answers to Supplementary Problems

7.53. (*a*) $A \cup B^c$; (*b*) $A \cap B^c$.

7.54. (*a*) $A \cap B \cap C^c$; (*b*) $(A \cup C) \cap B$; (*c*) $(A \cup B \cup B)^c = A^c \cap B^c \cap C^c$;
(*d*) $(A \cap B) \cup (A \cap C) \cup (B \cap C)$.

7.55. (*a*) $n(S) = 24$; $S = \{\text{H}, \text{T}\} \times \{\text{H}, \text{T}\} \times \{1, 2, \ldots, 6\}$.
(*b*) $A = \{\text{HH2, HH4, HH6}\}$; $B = \{\text{HH2, HT2, TH2, TT2}\}$;
$C = \{\text{HT1, HT3, HT5, TH1, TH3, TH5}\}$.
(*c*) (i) HH2; (ii) HT2, TH2, TT2; (iii) $\varnothing$.

7.56. (*a*) $\frac{3}{6}$; (*b*) $\frac{15}{16}$; (*c*) $\frac{20}{36}$.

7.57. (*a*) $\frac{8}{18}$; (*b*) $\frac{3}{18}$; (*c*) $\frac{5}{18}$.

7.58. (*a*) $\frac{40}{50}$; (*b*) $\frac{10}{50;}$ (*c*) $\frac{8}{150}$; (*d*) $\frac{42}{50}$.

7.59. (*a*) $\frac{1}{15}$; (*b*) $\frac{7}{15}$; (*c*) $\frac{8}{15}$; (*d*) $\frac{7}{15}$.

7.60. (*a*) $\frac{3}{10}$; (*b*) $\frac{3}{10}$; (*c*) $\frac{1}{15}$; (*d*) $\frac{8}{15}$.

7.61. $\frac{3}{5}$.

7.62. $\frac{1}{5}$.

7.63. (*a*) $3/4$; (*b*) $\frac{1}{4}$; (*c*) $\frac{1}{3}$; (*d*) $\frac{7}{12}$.

7.64. (*a*) $[4(3!)\,(3!)]/6! = \frac{1}{5}$; (*b*) $[2(3!)(3!)]/6! = \frac{1}{10}$.

7.65. (c) and (d).

7.66. $P(H) = \frac{3}{4}$; $P(T) = \frac{1}{4}$.

7.67. (a) $\frac{2}{5}$; (b) $\frac{1}{5}$; (c) $\frac{3}{5}$.

7.68. (a) 0.6, 0.8, 0.5; (b) 0.5, 0.7, 0.4.

7.69. (a) 0.3; (b) 0.8; (c) 0.2; (d) 0.2.

7.70. (a) 0.5; (b) 0.1; (c) 0.2; (d) 0.5.

7.71. (a) $\frac{1}{6}$, $\frac{5}{6}$; (b) $\frac{1}{2}$, $\frac{1}{3}$; (c) $\frac{1}{2}$, $\frac{2}{3}$; (d) $\frac{1}{2}$, 1; (e) yes, yes, no.

7.72. (a) $\frac{12}{30}$; (b) $\frac{4}{30}$.

7.73. (a) 0.7; (b) $\frac{2}{3}$; (c) $\frac{1}{3}$.

7.74. (a) $\frac{1}{3}$, $\frac{1}{4}$; (b) yes.

7.75. (a) 0.2; (b) $\frac{2}{7}$; (c) 0.5.

7.76. (a) 0.12, 0.58; (b) $\frac{3}{10}$, $\frac{4}{10}$.

7.77. (a) 20%; (b) $\frac{1}{3}$; (c) $\frac{1}{2}$.

7.78. (a) $\frac{1}{4}$; (b) $\frac{7}{12}$.

7.79. (a) $\frac{3}{4}$; (b) $\frac{1}{3}$.

7.80. Only (A, B).

7.81. (a) 0.16; (b) 0.18.

7.82. (a) $6(0.3)^2(0.7)^2 = 0.2646$, (b) $1 - (0.7)^4 = 0.7599$.

7.83. (a) $10(0.4)^2(0.6)^3 = 0.2646$; ($b$) $1 - (0.6)^5 = 0.7599$.

7.84. (b) P(WW, WT, TW) = 0.55.

7.85. (a) $1 - (\frac{2}{3})^3 = \frac{19}{27}$; ($b$) five times.

7.86.

x_i	1	2	3	4	5	6
p_i	$\frac{11}{36}$	$\frac{9}{16}$	$\frac{7}{36}$	$\frac{5}{36}$	$\frac{3}{36}$	$\frac{1}{36}$

$E(X) = \frac{91}{36} \approx 2.5$.

7.87.

x_i	0	1	2	3	4
p_i	$\frac{1}{16}$	$\frac{7}{16}$	$\frac{5}{16}$	$\frac{2}{16}$	$\frac{1}{16}$

$E(X) = \frac{27}{16} \approx 1.7$.

7.88. $\frac{211}{81} \approx 2.6$.

7.89. $\frac{23}{8} \approx 2.9$.

7.90. $\frac{11}{9} \approx 1.2$.

7.91. (*a*) 0.75; (*b*) -0.25.

7.92. 0.25.

7.93. (*a*) $\mu = 4$, $\sigma^2 = 5.5$, $\sigma = 2.3$; (*b*) $\mu = 1$, $\sigma^2 = 2.4$, $\sigma = 1.5$.

7.94. $\mu = ap + bq$; $\sigma^2 = pq(a-b)^2$; $\sigma = |a-b|\sqrt{pq}$.

7.95. (*a*)

x_i	2	3	4	5
$P(x_i)$	0.1	0.4	0.3	0.2

$E(X) = 3.6$; $\text{Var}(X) = 0.84$; $\sigma_X = 0.9$.

(*b*)

y_i	1	2	3
$P(y_i)$	0.1	0.5	0.4

$E(Y) = 2.3$; $\text{Var}(Y) = 0.41$; $\sigma_Y = 0.64$.

(*c*)

z_k	3	5	6	7	8
$P(z_k)$	0.1	0.4	0.1	0.2	0.2

$E(Z) = 5.9$; $\text{Var}(Z) = 2.3$; $\sigma_Z = 1.5$.

(*d*)

w_k	2	6	8	12	15
$P(w_k)$	0.1	0.4	0.1	0.2	0.2

$E(W) = 8.8$; $\text{Var}(W) = 17.6$; $\sigma_W = 4.2$.

7.96. $\mu = 80$; $\sigma^2 = 16$; $\sigma = 4$.

7.97. $\frac{6}{32} = \frac{3}{16}$.

7.98. $n = 6$; $p = \frac{1}{3}$.

© The McGraw–Hill Companies, 2004

Chapter 8

Graph Theory

8.1 INTRODUCTION, DATA STRUCTURES

Graphs, directed graphs, and trees and binary trees appear in many areas of mathematics and computer science. This and the next two chapters will cover these topics. However, in order to understand how these objects may be stored in memory and to understand algorithms on them, we need to know a little about certain data structures. We assume the reader does understand linear and two-dimensional arrays; hence we will only discuss linked lists and pointers, and stacks and queues below.

Linked Lists and Pointers

Linked lists and pointers will be introduced by means of an example. Suppose a brokerage firm maintains a file in which each record contains a customer's name and salesman; say the file contains the following data:

Customer	Adams	Brown	Clark	Drew	Evans	Farmer	Geller	Hill	Infeld
Salesman	Smith	Ray	Ray	Jones	Smith	Jones	Ray	Smith	Ray

There are two basic operations that one would want to perform on the data:

Operation A: Given the name of a customer, find his salesman.

Operation B: Given the name of a salesman, find the list of his customers.

We discuss a number of ways the data may be stored in the computer, and the ease with which one can perform the operations A and B on the data.

Clearly, the file could be stored in the computer by an array with two rows (or columns) of nine names. Since the customers are listed alphabetically, one could easily perform Operation A. However, in order to perform operation B one must search through the entire array.

One can easily store the data in memory using a two-dimensional array where, say, the rows correspond to an alphabetical listing of the customers and the columns correspond to an alphabetical listing of the salesmen, and where there is a 1 in the matrix indicating the salesman of a customer and there are 0s elsewhere. The main drawback of such a representation is that there may be a waste of a lot of memory because many 0s may be in the matrix. For example, if a firm has 1000 customers and 20 salesmen, one would need 20 000 memory locations for the data, but only 1000 of them would be useful.

We discuss below a way of storing the data in memory which uses linked lists and pointers. By a *linked list*, we mean a linear collection of data elements, called *nodes*, where the linear order is given by means of a field of pointers. Figure 8-1 is a schematic diagram of a linked list with six nodes. That is, each node is divided into two parts: the first part contains the information of the element (e.g., NAME, ADDRESS, ...), and the second part, called the *link field* or *nextpointer field*, contains the address of the next node in the list. This pointer field is indicated by an arrow drawn from one node to the next node in the list. There is also a variable pointer, called START in Fig. 8-1, which gives the address of the first node in the list. Furthermore, the pointer field of the last node contains an invalid address, called a *null pointer*, which indicates the end of the list.

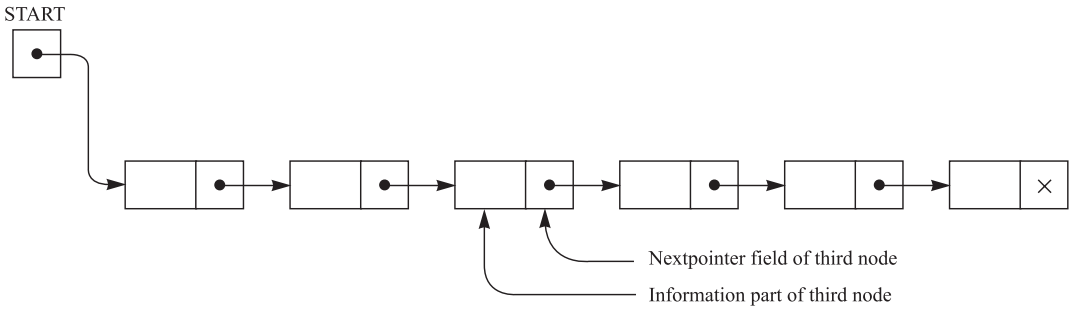


Fig. 8-1 Linked list with 6 nodes.

One main way of storing the original data, pictured in Fig. 8-2, uses linked lists. Observe that there are separate (sorted alphabetically) arrays for the customers and the salesmen. Also, there is a pointer array SLSM parallel to CUSTOMER which gives the location of the salesman of a customer; hence operation *A* can be performed very easily and quickly. Furthermore, the list of customers of each salesman is a linked list as discussed above. Specifically, there is a pointer array START parallel to SALESMAN which points to the first customer of a salesman, and there is a array NEXT which points to the location of the next customer in the salesman's list (or contains a 0 to indicate the end of the list). This process is indicated by the arrows in Fig. 8-2 for the salesman Ray.

	Customer	SLSM	NEXT
1	Adams	3	5
2	Brown	2	3
3	Clark	2	7
4	Drew	1	6
5	Evans	3	8
6	Farmer	1	0
7	Geller	2	9
8	Hill	3	0
9	Infeld	2	0

Salesman	START	
Jones	4	1
Ray	2	2
Smith	1	4

Fig. 8-2

Operation *B* can now be performed easily and quickly; that is, one does not need to search through the list of all customers in order to obtain the list of customers of a given salesman. The following is such an algorithm (which is written in pseudocode).

Algorithm 8.1 The name of a salesman is read and the list of his customers is printed.

Step 1. Read XXX.

Step 2. Find *K* such that SALESMAN[K] = XXX. [Use binary search.]

Step 3. Set PTR := START[*K*]. [Initializes pointer PTR.]

Step 4. Repeat while PTR $\neq$ NULL.

(*a*) Print CUSTOMER[PTR].

(*b*) Set PTR := NEXT[PTR]. [Update PTR.]

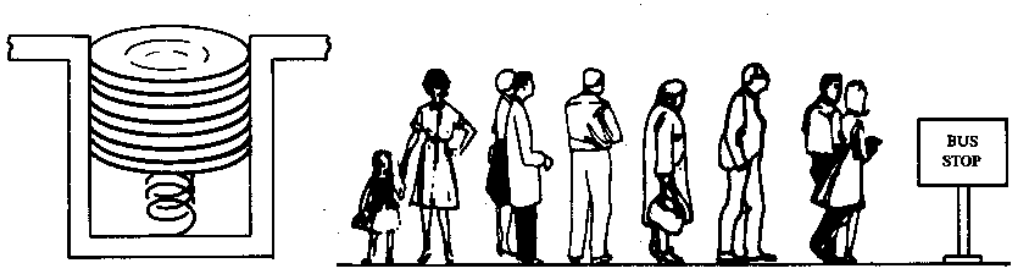
[End of loop.]

Step 5. Exit.

Stacks, Queues, and Priority Queues

There are data structures other than arrays and linked lists which will occur in our graph algorithms. These structures, stacks, queues, and priority queues, are briefly described below.

(*a*) ***Stack***: A *stack*, also called a *last-in first-out* (LIFO) system, is a linear list in which insertions and deletions can take place only at one end, called the "top" of the list. This structure is similar in its operation to a stack of dishes on a spring system, as pictured in Fig. 8-3(*a*). Note that new dishes are inserted only at the top of the stack and dishes can be deleted only from the top of the stack.



(*a*) Stack of dishes. (*b*) Queue waiting for a bus.

Fig. 8-3

(*b*) ***Queue***: A *queue*, also called a *first-in first-out* (FIFO) system, is a linear list in which deletions can only take place at one end of the list, the "front" of the list, and insertions can only take place at the other end of the list, the "rear" of the list. The structure operates in much the same way as a line of people waiting at a bus stop, as pictured in Fig. 8-3(*b*). That is, the first person in line is the first person to board the bus, and a new person goes to the end of the line.

(*c*) ***Priority queue***: Let S be a set of elements where new elements may be periodically inserted, but where the current largest element (element with the "highest priority") is always deleted. Then S is called a *priority queue*. The rules "women and children first" and "age before beauty" are examples of priority queues. Stacks and ordinary queues are special kinds of priority queues. Specifically, the element with the highest priority in a stack is the last element inserted, but the element with the highest priority in a queue is the first element inserted.

8.2 GRAPHS AND MULTIGRAPHS

A *graph* G consists of two things:

(i) A set $V = V(G)$ whose elements are called *vertices*, *points*, or *nodes* of G.

(ii) A set $E = E(G)$ of unordered pairs of distinct vertices called *edges* of G.

We denote such a graph by $G(V, E)$ when we want to emphasize the two parts of G.

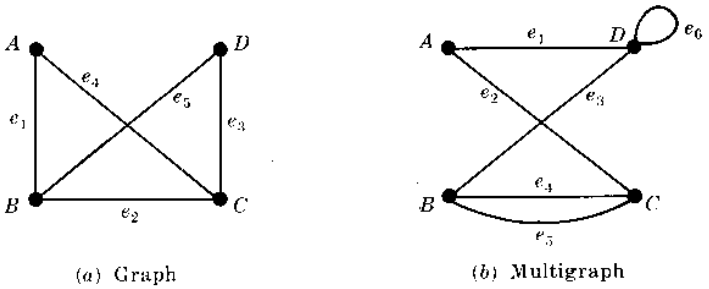
Vertices u and v are said to be *adjacent* if there is an edge $e = \{u, v\}$. In such a case, u and v are called the *endpoints* of e, and e is said to *connect* u and v. Also, the edge e is said to be *incident* on each of its endpoints u and v.

Graphs are pictured by diagrams in the plane in a natural way. Specifically, each vertex v in V is represented by a dot (or small circle), and each edge $e = \{v_1, v_2)\}$ is represented by a curve which connects its endpoints v_1 and v_2. For example, Fig. 8-4(*a*) represents the graph $G(V, E)$ where:

(i) V consists of vertices A, B, C, D.

(ii) E consists of edges $e_1 = \{A, B\}$, $e_2 = \{B, C\}$, $e_3 = \{C, D\}$, $e_4 = \{A, C\}$, $e_5 = \{B, D\}$.

In fact, we will usually denote a graph by drawing its diagram rather than explicitly listing its vertices and edges.



(a) Graph (b) Multigraph

Fig. 8-4

Multigraphs

Consider the diagram in Fig. 8-4(*b*). The edges e_4 and e_5 are called *multiple edges* since they connect the same endpoints, and the edge e_6 is called a *loop* since its endpoints are the same vertex. Such a diagram is called a *multigraph*; the formal definition of a graph permits neither multiple edges nor loops. Thus a graph may be defined to be a multigraph without multiple edges or loops.

Remark: Some texts use the term *graph* to include multigraphs and use the term *simple graph* to mean a graph without multiple edges and loops.

Degree of a Vertex

The *degree* of a vertex v in a graph G, written deg (v), is equal to the number of edges in G which contain v, that is, which are incident on v. Since each edge is counted twice in counting the degrees of the vertices of G, we have the following simple by important result.

Theorem 8.1: The sum of the degrees of the vertices of a graph G is equal to twice the number of edges in G.

Consider, for example, the graph in Fig. 8-4(*a*). We have

$$\deg(A) = 2, \qquad \deg(B) = 3, \qquad \deg(C) = 3, \qquad \deg(D) = 2$$

The sum of the degrees equals 10 which, as expected, is twice the number of edges. A vertex is said to be *even* or *odd* according as its degree is an even or an odd number. Thus A and D are even vertices whereas B and C are odd vertices.

Theorem 8.1 also holds for multigraphs where a loop is counted twice toward the degree of its endpoint. For example, in Fig. 8-4(*b*) we have deg $(D) = 4$ since the edge e_6 is counted twice; hence D is an even vertex.

A vertex of degree zero is called an *isolated* vertex.

Finite Graphs, Trivial Graph

A multigraph is said to be *finite* if it has a finite number of vertices and a finite number of edges. Observe that a graph with a finite number of vertices must automatically have a finite number of edges and so must be finite. The finite graph with one vertex and no edges, i.e., a single point, is called the *trivial graph*. Unless otherwise specified, the multigraphs in this book shall be finite.

8.3 SUBGRAPHS, ISOMORPHIC AND HOMEOMORPHIC GRAPHS

This section will discuss important relationships between graphs.

Subgraphs

Consider a graph $G = G(V, E)$. A graph $H = H(V', E')$ is called a *subgraph* of G if the vertices and edges of H are contained in the vertices and edges of G, that is, if $V' \subseteq V$ and $E' \subseteq E$. In particular:

(i) A subgraph $H(V', E')$ of $G(V, E)$ is called the subgraph *induced* by its vertices V' if its edge set E' contains all edges in G whose endpoints belong to vertices in H.

(ii) If v is a vertex in G, then $G - v$ is the subgraph of G obtained by deleting v from G and deleting all edges in G which contain v.

(iii) If e is an edge in G, then $G - e$ is the subgraph of G obtained by simply deleting the edge e from G.

Isomorphic Graphs

Graphs $G(V, E)$ and $G^*(V^*, E^*)$ are said to be *isomorphic* if there exists a one-to-one correspondence $f: V \to V^*$ such that $\{u, v\}$ is an edge of G if and only if $\{f(u), f(v)\}$ is an edge of G^*. Normally, we do not distinguish between isomorphic graphs (even though their diagrams may "look different"). Fig. 8-5 gives ten graphs pictured as letters. We note that A and R are isomorphic graphs. Also, F and T, K and X, and M, S, V, and Z are isomorphic graphs.

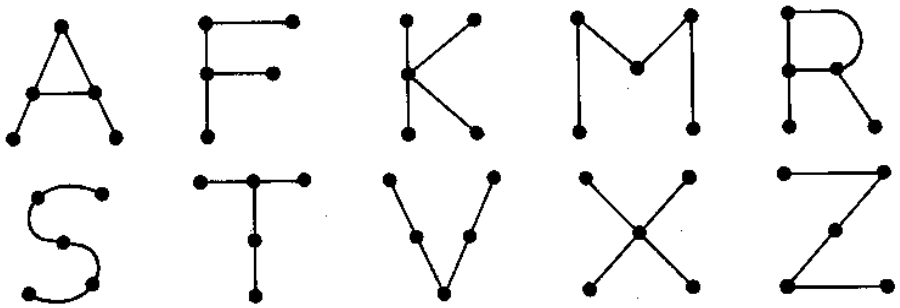


Fig. 8-5

Homeomorphic Graphs

Given any graph G, we can obtain a new graph by dividing an edge of G with additional vertices. Two graphs G and G^* are said to *homeomorphic* if they can be obtained from the same graph or isomorphic graphs by this method. The graphs (a) and (b) in Fig. 8-6 are not isomorphic, but they are homoeomorphic since they can be obtained from the graph (c) by adding appropriate vertices.

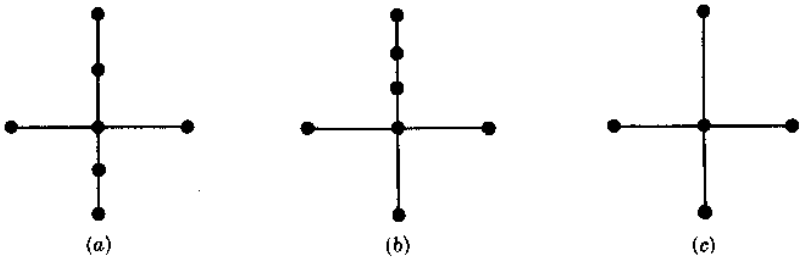


Fig. 8-6

8.4 PATHS, CONNECTIVITY

A *path* in a multigraph G consists of an alternating sequence of vertices and edges of the form

$$v_0, \quad e_1, \quad v_1, \quad e_2, \quad v_2, \quad \ldots, \quad e_{n-1}, \quad v_{n-1}, \quad e_n, \quad v_n$$

where each edge e_i contains the vertices v_{i-1} and v_i (which appear on the sides of e_i in the sequence). The number n of edges is called the *length* of the path. When there is no ambiguity, we denote a path by its sequence of vertices $(v_0, v_1, \ldots, v_n)$. The path is said to be *closed* if $v_0 = v_n$. Otherwise, we say the path is from v_0 *to* v_n, or *between* v_0 and v_n, or *connects* v_0 to v_n.

A *simple path* is a path in which all vertices are distinct. (A path in which all edges are distinct will be called a *trail*.) A *cycle* is a closed path of length 3 or more in which all vertices are distinct except $v_0 = v_n$. A cycle of length k is called a *k-cycle*.

EXAMPLE 8.1 Consider the graph G in Fig. 8-7(a). Consider the following sequences:

$$\alpha = (P_4, P_1, P_2, P_5, P_1, P_2, P_3, P_6), \qquad \beta = (P_4, P_1, P_5, P_2, P_6),$$
$$\gamma = (P_4, P_1, P_5, P_2, P_3, P_5, P_6), \qquad \delta = (P_4, P_1, P_5, P_3, P_6).$$

The sequence α is a path from P_4 to P_6; but it is not a trail since the edge $\{P_1, P_2\}$ is used twice. The sequence β is not a path since there is no edge $\{P_2, P_6\}$. The sequence γ is a trail since no edge is used twice; but it is not a simple path since the vertex P_5 is used twice. The sequence δ is a simple path from P_4 to P_6; but it is not the shortest path (with respect to length) from P_4 to P_6. The shortest path from P_4 to P_6 is the simple path (P_4, P_5, P_6) which has length 2.

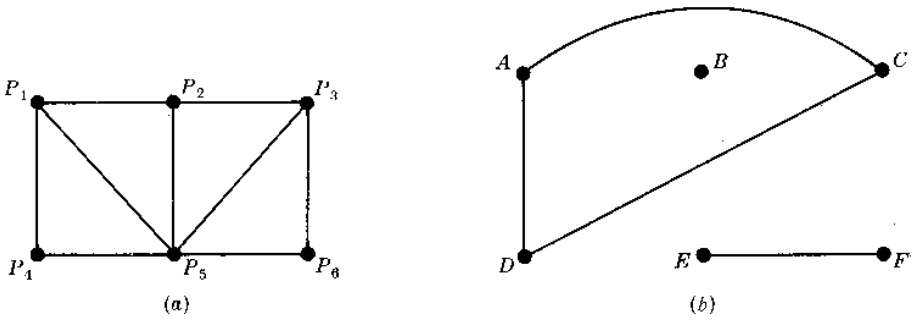


Fig. 8-7

By eliminating unnecessary edges, it is not difficult to see that any path from a vertex u to a vertex v can be replaced by a simple path from u to v. We state this result formally.

Theorem 8.2: There is a path from a vertex u to a vertex v if and only if there exists a simple path from u to v.

Connectivity, Connected Components

A graph G is *connected* if there is a path between any two of its vertices. The graph in Fig. 8-7(a) is connected, but the graph in Fig. 8-7(b) is not connected since, for example, there is no path between vertices D and E.

Suppose G is a graph. A connected subgraph H of G is called a *connected component* of G if H is not contained in any larger connected subgraph of G. It is intuitively clear that any graph G can be partitioned into its connected components. For example, the graph G in Fig. 8-7(b) has three connected components, the subgraphs induced by the vertex sets $\{A, C, D\}$, $\{E, F\}$, and $\{B\}$.

The vertex B in Fig. 8-7(b) is called an *isolated vertex* since B does not belong to any edge or, in other words, deg $(B) = 0$. Therefore, as noted, B itself forms a connected component of the graph.

Remark: Formally speaking, assuming any vertex u is connected to itself, the relation "u is connected to v" is an equivalence relation on the vertex set of a graph G and the equivalence classes of the relation form the connected components of G.

Distance and Diameter

Consider a connected graph G. The *distance* between vertices u and v in G, written $d(u,v)$, is the length of the shortest path between u and v. The *diameter* of G, written $\text{diam}(G)$, is the maximum distance between any two points in G. For example, in Fig. 8-8(a), $d(A,F) = 2$ and $\text{diam}(G) = 3$, whereas in Fig. 8-8(b), $d(A,F) = 3$ and $\text{diam}(G) = 4$.

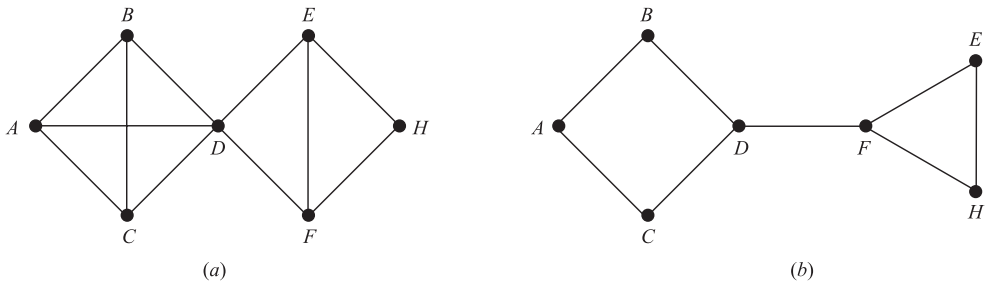


Fig. 8-8

Cutpoints and Bridges

Let G be a connected graph. A vertex v in G is called a *cutpoint* if $G - v$ is disconnected. (Recall that $G - v$ is the graph obtained from G by deleting v and all edges containing v.) An edge e of G is called a *bridge* if $G - e$ is disconnected. (Recall that $G - e$ is the graph obtained from G by simply deleting the edge e). In Fig. 8-8(a), the vertex D is a cutpoint and there are no bridges. In Fig. 8-8(b), the edge $e = \{D, F\}$ is a bridge. (Its endpoints D and F are necessarily cutpoints.)

8.5 THE BRIDGES OF KÖNIGSBERG, TRAVERSABLE MULTIGRAPHS

The eighteenth-century East Prussian town of Königsberg included two islands and seven bridges as shown in Fig. 8-9(a). Question: Beginning anywhere and ending anywhere, can a person walk through town crossing all seven bridges but not crossing any bridge twice? The people of Königsberg wrote to the celebrated Swiss mathematician L. Euler about this question. Euler proved in 1736 that such a walk is impossible. He replaced the islands and the two sides of the river by points and the bridges by curves, obtaining Fig. 8-9(b).

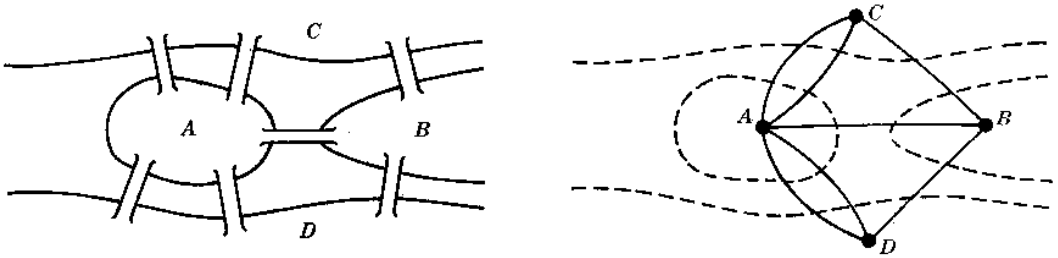


Fig. 8-9

Observe that Fig. 8-9(*b*) is a multigraph. A multigraph is said to be *traversable* if it "can be drawn without any breaks in the curve and without repeating any edges", that is, if there is a path which includes all vertices and uses each edge exactly once. Such a path must be a trail (since no edge is used twice) and will be called a *traversable trail*. Clearly a traversable multigraph must be finite and connected. Figure 8-10(*b*) shows a traversable trail of the multigraph in Fig. 8-10(*a*). (To indicate the direction of the trail, the diagram misses touching vertices which are actually traversed.) Now it is not difficult to see that the walk in Königsberg is possible if and only if the multigraph in Fig. 8-9(*b*) is traversable.

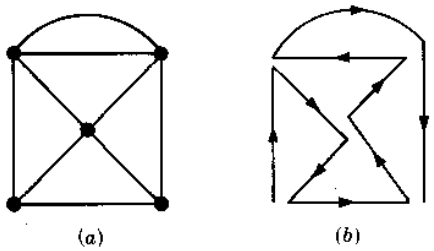


Fig. 8-10

We now show how Euler proved that the multigraph in Fig. 8-9(*b*) is not traversable and hence that the walk in Königsberg is impossible. Recall first that a vertex is even or odd according as its degree is an even or an odd number. Suppose a multigraph is traversable and that a traversable trail does not begin or end at a vertex P. We claim that P is an even vertex. For whenever the traversable trail enters P by an edge, there must always be an edge not previously used by which the trail can leave P. Thus the edges in the trail incident with P must appear in pairs, and so P is an even vertex. Therefore if a vertex Q is odd, the traversable trail must begin or end at Q. Consequently, a multigraph with more than two odd vertices cannot be traversable. Observe that the multigraph corresponding to the Königsberg bridge problem has four odd vertices. Thus one cannot walk through Königsberg so that each bridge is crossed exactly once.

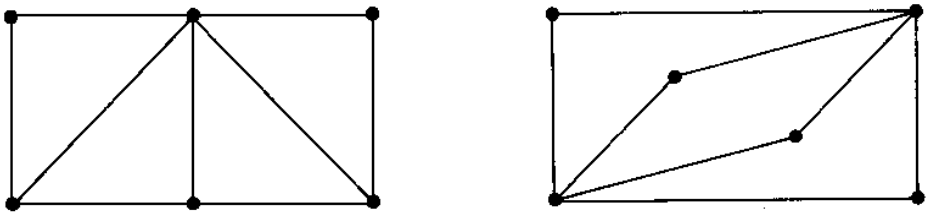
Euler actually proved the converse of the above statement, which is contained in the following theorem and corollary. (The theorem is proved in Problem 8.9.) A graph G is called an *Eulerian* graph if there exists a closed traversable trail, called an *Eulerian* trail.

Theorem 8.3 (Euler): A finite connected graph is Eulerian if and only if each vertex has even degree.

Corollary 8.4: Any finite connected graph with two odd vertices is traversable. A traversable trail may begin at either odd vertex and will end at the other odd vertex.

Hamiltonian Graphs

The above discussion of Eulerian graphs emphasized traveling edges; here we concentrate on visiting vertices. A *Hamiltonian circuit* in a graph G, named after the nineteenth-century Irish mathematician William Hamilton (1805–1865), is a closed path that visits every vertex in G exactly once. (Such a closed path must be a cycle.) If G does admit a Hamiltonian circuit, then G is called a *Hamiltonian graph*. Note that an Eulerian circuit traverses every edge exactly once, but may repeat vertices, while a Hamiltonian circuit visits each vertex exactly once but may repeat edges. Figure 8-11 gives an example of a graph which is Hamiltonian but not Eulerian, and vice versa.



(*a*) Hamiltonian and non-Eulerian (*b*) Eulerian and non-Hamiltonian

Fig. 8-11

Although it is clear that only connected graphs can be Hamiltonian, there is no simple criterion to tell us whether or not a graph is Hamiltonian as there is for Eulerian graphs. We do have the following sufficient condition which is due to G. A. Dirac.

Theorem 8.5: Let G be a connected graph with n vertices. Then G is Hamiltonian if $n \geq 3$ and $n \leq \deg(v)$ for each vertex v in G.

8.6 LABELED AND WEIGHTED GRAPHS

A graph G is called a *labeled graph* if its edges and/or vertices are assigned data of one kind or another. In particular, G is called a *weighted graph* if each edge e of G is assigned a nonnegative number $w(e)$ called the *weight* or *length* of v. Figure 8-12 shows a weighted graph where the weight of each edge is given in the obvious way. The *weight* (or *length*) of a path in such a weighted graph G is defined to be the sum of the weights of the edges in the path. One important problem in graph theory is to find a *shortest path*, that is, a path of minimum weight (length), between any two given vertices. The length of a shortest path between P and Q in Fig. 8-12 is 14; one such path is

$$(P, A_1, A_2, A_5, A_3, A_6, Q)$$

The reader can try to find another shortest path.

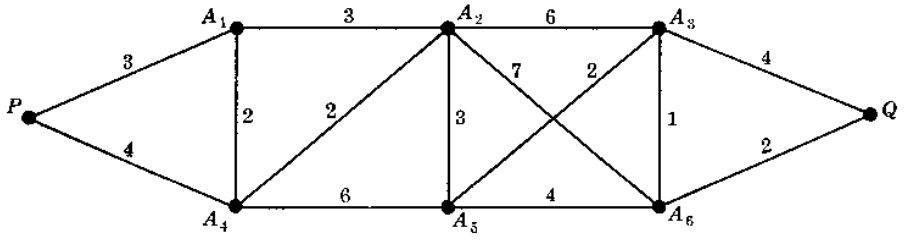


Fig. 8-12

8.7 COMPLETE, REGULAR, AND BIPARTITE GRAPHS

There are many different types of graphs. This section considers three of them, complete, regular, and bipartite graphs.

Complete Graphs

A graph G is said to be *complete* if every vertex in G is connected to every other vertex in G. Thus a complete graph G must be connected. The complete graph with n vertices is denoted by K_n. Figure 8-13 shows the graphs K_1 through K_6.

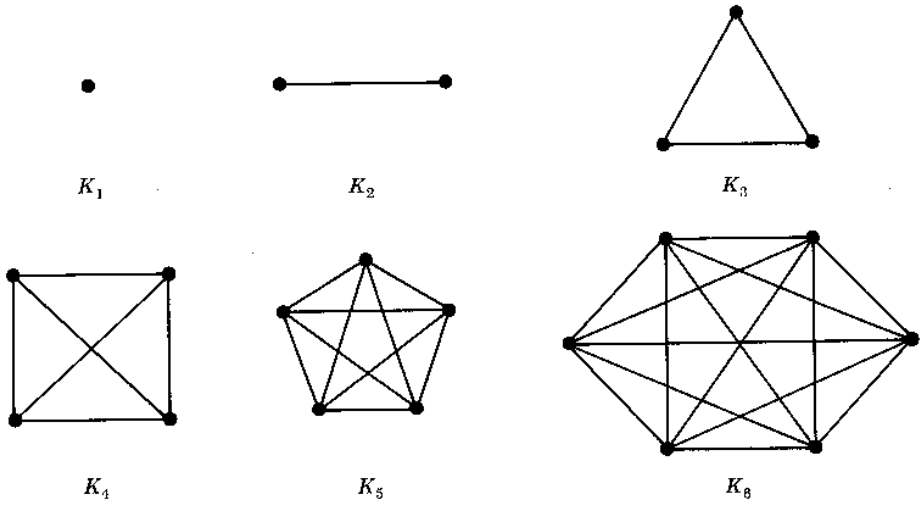


Fig. 8-13

Regular Graphs

A graph G is *regular of degree* k or *k-regular* if every vertex has degree k. In other words, a graph is regular if every vertex has the same degree.

The connected regular graphs of degrees 0, 1, or 2 are easily described. The connected 0-regular graph is the trivial graph with one vertex and no edges. The connected 1-regular graph is the graph with two vertices and one edge connecting them. The connected 2-regular graph with n vertices is the graph which consists of a single n-cycle.

See Fig. 8-14.

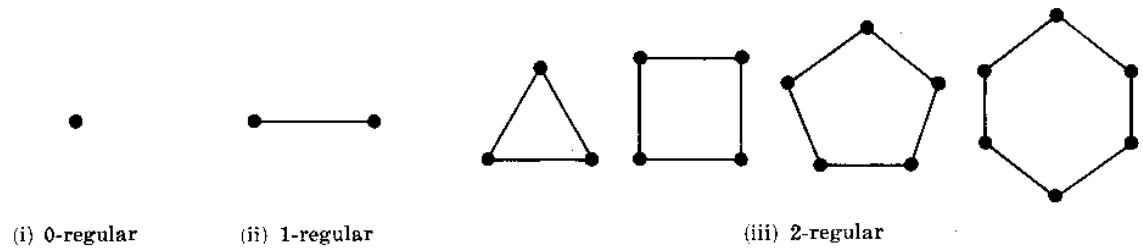


Fig. 8-14 Regular graphs.

The 3-regular graphs must have an even number of vertices since the sum of the degrees of the vertices is an even number (Theorem 8.1). Figure 8-15 shows two connected 3-regular graphs with six vertices. In general, regular graphs can be quite complicated. For example, there are nineteen 3-regular graphs with ten vertices. We note that the complete graph with n vertices K_n is regular of degree $n - 1$.

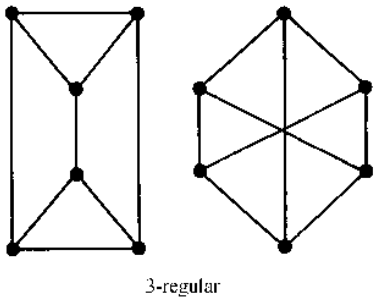


Fig. 8-15

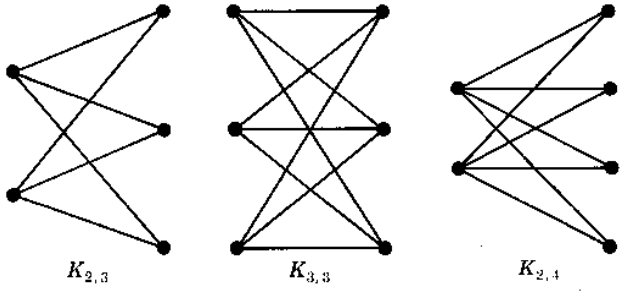


Fig. 8-16

Bipartite Graphs

A graph G is said to be *bipartite* if its vertices V can be partitioned into two subsets M and N such that each edge of G connects a vertex of M to a vertex of N. By a complete bipartite graph, we mean that each vertex of M is connected to each vertex of N; this graph is denoted by $K_{m,n}$ where m is the number of vertices in M and n is the number of vertices in N, and, for standardization, we will assume $m \leq n$. Figure 8-16 shows the graphs $K_{2,3}$, $K_{3,3}$, and $K_{2,4}$, Clearly the graph $K_{m,n}$ has mn edges.

8.8 TREE GRAPHS

A graph T is called a *tree* if T is connected and T has no cycles. Examples of trees are shown in Fig. 8-17. A *forest* G is a graph with no cycles; hence the connected components of a forest G are trees. [A graph without cycles is said to be *cycle-free*.] The tree consisting of a single vertex with no edges is called the *degenerate tree*.

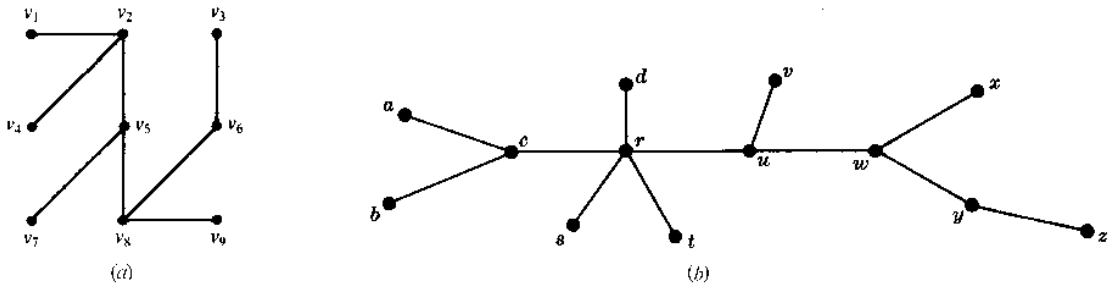


Fig. 8-17

Consider a tree T. Clearly, there is only one simple path between two vertices of T; otherwise, the two paths would form a cycle. Also:

(*a*) Suppose there is no edge $\{u, v\}$ in T and we add the edge $e = \{u, v\}$ to T. Then the simple path from u to v in T and e will form a cycle; hence T is no longer a tree.

(*b*) On the other hand, suppose there is an edge $e = \{u, v\}$ in T, and we delete e from T. Then T is no longer connected (since there cannot be a path from u to v); hence T is no longer a tree.

The following theorem (proved in Problem 8.16) applies when our graphs are finite.

Theorem 8.6: Let G be a graph with $n > 1$ vertices. Then the following are equivalent:

(i) G is a tree.

(ii) G is a cycle-free and has $n - 1$ edges.

(iii) G is connected and has $n - 1$ edges.

This theorem also tells us that a finite tree T with n vertices must have $n - 1$ edges. For example, the tree in Fig. 8-17(a) has 9 vertices and 8 edges, and the tree in Fig. 8-17(b) has 13 vertices and 12 edges.

Spanning Trees

A subgraph T of a connected graph G is called a *spanning tree* of G if T is a tree and T includes all the vertices of G. Figure 8-18 shows a connected graph G and spanning trees T_1, T_2, and T_3 of G.

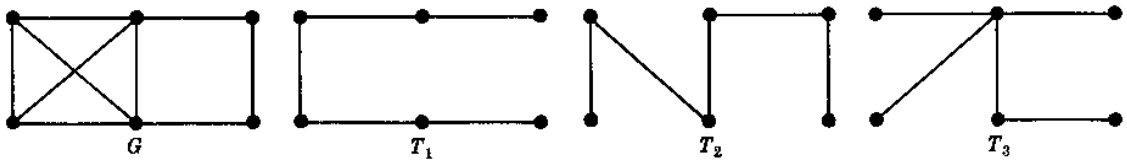


Fig. 8-18

Minimum Spanning Trees

Suppose G is a connected weighted graph. That is, each edge of G is assigned a nonnegative number called the *weight* of the edge. Then any spanning tree T of G is assigned a total weight obtained by adding the weights of the edges in T. A *minimal spanning tree* of G is a spanning tree whose total weight is as small as possible.

Algorithms 8.8A and 8.8B, which follow, enable us to find a minimal spanning tree T of a connected weighted graph G where G has n vertices. (In which case T must have $n - 1$ edges.)

Algorithm 8.8A: The input is a connected weighted graph G with n vertices.

Step 1. Arrange the edges of G in the order of decreasing weights.

Step 2. Proceeding sequentially, delete each edge that does not disconnect the graph until $n - 1$ edges remain.

Step 3. Exit.

Algorithm 8.8B (Kruskal): The input is a connected weighted graph G with n vertices.

Step 1. Arrange the edges of G in order of increasing weights.

Step 2. Starting only with the vertices of G and proceeding sequentially, add each edge which does not result in a cycle until $n - 1$ edges are added.

Step 3. Exit.

The weight of a minimal spanning tree is unique, but the minimal spanning tree itself is not. Different minimal spanning trees can occur when two or more edges have the same weight. In such a case, the arrangement of the edges in Step 1 of Algorithms 8.8A or 8.8B is not unique and hence may result in different minimal spanning trees as illustrated in the following example.

EXAMPLE 8.2 Find a minimal spanning tree of the weighted graph Q in Fig. 8-19(a). Note that Q has six vertices, so a minimal spanning tree will have five edges.

(a) Here we apply Algorithm 8.8A.

First we order the edges by decreasing weights, and then we successively delete edges without disconnecting Q until five edges remain. This yields the following data:

Edges	BC	AF	AC	BE	CE	BF	AE	DF	BD
Weight	8	7	7	7	6	5	4	4	3
Delete?	Yes	Yes	Yes	No	No	Yes			

Thus the minimal spanning tree of Q which is obtained contains the edges

$$BE, \quad CE, \quad AE, \quad DF, \quad BD$$

The spanning tree has weight 24 and it is shown in Fig. 8-19(b).

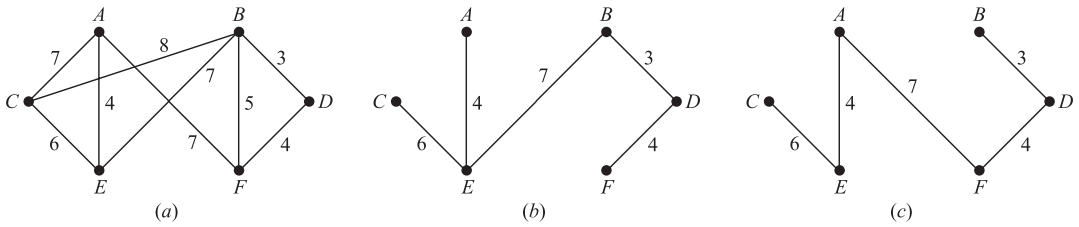


Fig. 8-19

(b) Here we apply Algorithm 8.8B.

First we order the edges by increasing weights, and then we successively add edges without forming any cycles until five edges are included. This yields the following data:

Edges	BD	AE	DF	BF	CE	AC	AF	BE	BC
Weight	3	4	4	5	6	7	7	7	8
Add?	Yes	Yes	Yes	No	Yes	No	Yes		

Thus the minimal spanning tree of Q which is obtained contains the edges

$$BD, \quad AE, \quad DF, \quad CE, \quad AF$$

The spanning tree appears in Fig. 8-19(c). Observe that this spanning tree is not the same as the one obtained using Algorithm 8.8A.

Remark: The above algorithms are easily executed when the graph G is relatively small as in Fig. 8-19(a). Suppose G has dozens of vertices and hundreds of edges which, say, are given by a list of pairs of vertices. Then even deciding whether G is connected is not obvious; it may require some type of depth-first search (DFS) or breadth-first search (BFS) graph algorithm. Later sections and the next chapter will discuss ways of representing graphs G in memory and will discuss various graph algorithms.

8.9 PLANAR GRAPHS

A graph or multigraph which can be drawn in the plane so that its edges do not cross is said to be *planar*. Although the complete graph with four vertices K_4 is usually pictured with crossing edges as in Fig. 8-20(a), it can also be drawn with noncrossing edges as in Fig. 8-20(b); hence K_4 is planar. Tree

graphs form an important class of planar graphs. This section introduces our reader to these important graphs.

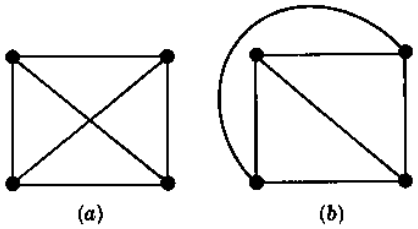


Fig. 8-20

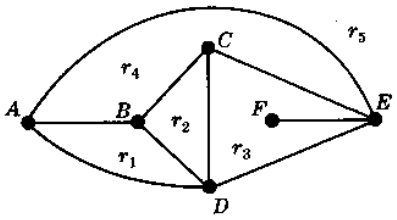


Fig. 8-21

Maps, Regions

A particular planar representation of a finite planar multigraph is called a *map*. We say that the map is *connected* if the underlying multigraph is connected. A given map divides the plane into various regions. For example, the map in Fig. 8-21 with six vertices and nine edges divides the plane into five regions. Observe that four of the regions are bounded, but the fifth region, outside the diagram, is unbounded. Thus there is no loss in generality in counting the number of regions if we assume that our map is contained in some large rectangle rather than in the entire plane.

Observe that the border of each region of a map consists of edges. Sometimes the edges will form a cycle, but sometimes not. For example, in Fig. 8-21 the borders of all the regions are cycles except for r_3. However, if we do move counterclockwise around r_3 starting, say, at the vertex C, then we obtain the closed path

$$(C, D, E, F, E, C)$$

where the edge $\{E, F\}$ occurs twice. By the *degree* of a region r, written deg (r), we mean the length of the cycle or closed walk which borders r. We note that each edge either borders two regions or is contained in a region and will occur twice in any walk along the border of the region. Thus we have a theorem for regions which is analogous to Theorem 8.1 for vertices.

Theorem 8.7: The sum of the degrees of the regions of a map is equal to twice the number of edges.

The degrees of the regions of Fig. 8-21 are:

$$\deg(r_1) = 3, \qquad \deg(r_2) = 3, \qquad \deg(r_3) = 5, \qquad \deg(r_4) = 4, \qquad \deg(r_5) = 3$$

The sum of the degrees is 18, which, as expected, is twice the number of edges.

For notational convenience we shall picture the vertices of a map with dots or small circles, or we shall assume that any intersections of lines or curves in the plane are vertices.

Euler's Formula

Euler gave a formula which connects the number V of vertices, the number E of edges, and the number R of regions of any connected map. Specifically:

Theorem 8.8 (Euler): $V - E + R = 2$.

(The proof of Theorem 8.8 appears in Problem 8.20.)

Observe that, in Fig. 8-21, $V = 6$, $E = 9$, and $R = 5$; and, as expected by Euler's formula.

$$V - E + R = 6 - 9 + 5 = 2$$

We emphasize that the underlying graph of a map must be connected in order for Euler's formula to hold.

Let G be a connected planar multigraph with three or more vertices, so G is neither K_1 nor K_2. Let M be a planar representation of G. It is not difficult to see that (1) a region of M can have degree 1 only if its border is a loop, and (2) a region of M can have degree 2 only if its border consists of two multiple edges. Accordingly, if G is a graph, not a multigraph, then every region of M must have degree 3 or more. This comment together with Euler's formula is used to prove the following result on planar graphs.

Theorem 8.9: Let G be a connected planar graph with p vertices and q edges, where $p \geq 3$. Then $q \geq 3p - 6$.

Note that the theorem is not true for K_1 where $p = 1$ and $q = 0$, and is not true for K_2 where $p = 2$ and $q = 1$.

Proof: Let r be the number of regions in a planar representation of G. By Euler's formula,

$$p - q + r = 2$$

Now the sum of the degrees of the regions equals $2q$ by Theorem 8.7. But each region has degree 3 or more; hence

$$2q \geq 3r$$

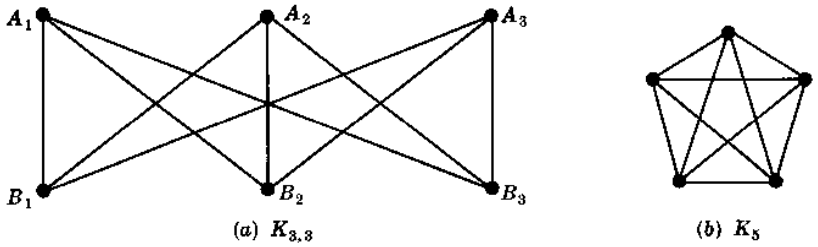
Thus $r \geq 2q/3$. Substituting this in Euler's formula gives

$$2 = p - q + r \leq p - q + \frac{2q}{3} \qquad \text{or} \qquad 2 \leq p - \frac{q}{3}$$

Multiplying the inequality by 3 gives $6 \leq 3p - q$ which gives us our result.

Nonplanar Graphs, Kuratowski's Theorem

We give two examples of nonplanar graphs. Consider first the *utility graph*; that is, three houses A_1, A_2, A_3 are to be connected to outlets for water, gas and electricity, B_1, B_2, B_3, as in Fig. 8-22(a). Observe that this is the graph $K_{3,3}$ and it has $p = 6$ vertices and $q = 9$ edges. Suppose the graph is planar. By Euler's formula a planar representation has $r = 5$ regions. Observe that no three vertices are connected to each other; hence the degree of each region must be 4 or more and so the sum of the degrees of the regions must be 20 or more. By Theorem 5.9 the graph must have 10 or more edges. This contradicts the fact that the graph has $q = 9$ edges. Thus the utility graph $K_{3,3}$ is nonplanar.



(a) $K_{3,3}$ (b) K_5

Fig. 8-22

Consider next the *star graph* in Fig. 8-22(b). This is the complete graph K_5 on $p = 5$ vertices and has $q = 10$ edges. If the graph is planar, then by Theorem 8.9.

$$10 = q \leq 3p - 6 = 15 - 6 = 9$$

which is impossible. Thus K_5 is nonplanar.

For many years mathematicians tried to characterize planar and nonplanar graphs. This problem was finally solved in 1930 by the Polish mathematician K. Kuratowski. The proof of this result, stated below, lies beyond the scope of this text.

Theorem 8.10 (Kuratowski): A graph is nonplanar if and only if it contains a subgraph homeomorphic to $K_{3,3}$ or K_5.

8.10 GRAPH COLORINGS

Consider a graph G. A *vertex coloring*, or simply a *coloring* of G is an assignment of colors to the vertices of G such that adjacent vertices have different colors. We say that G is n-colorable if there exists a coloring of G which uses n colors. (Since the word "color" is used as a noun, we will try to avoid its use as a verb by saying, for example, "paint" G rather than "color" G when we are assigning colors to the vertices of G.) The minimum number of colors needed to paint G is called the *chromatic number* of G and is denoted by $\chi(G)$.

We give an algorithm by Welch and Powell for a coloring of a graph G. We emphasize that this algorithm does not always yield a minimal coloring of G.

Algorithm 8.10 (Welch-Powell): The input is a graph G.

Step 1. Order the vertices of G according to decreasing degrees.

Step 2. Assign the first color C_1 to the first vertex and then, in sequential order, assign C_1 to each vertex which is not adjacent to a previous vertex which was assigned C_1.

Step 3. Repeat Step 2 with a second color C_2 and the subsequence of noncolored vertices.

Step 4. Repeat Step 3 with a third color C_3, then a fourth color C_4, and so on until all vertices are colored.

Step 5. Exit.

EXAMPLE 8.3

(*a*) Consider the graph G in Fig. 8-23. We use the Welch-Powell Algorithm 8.10 to obtain a coloring of G. Ordering the vertices according to decreasing degrees yields the following sequence:

$$A_5, \quad A_3, \quad A_7, \quad A_1, \quad A_2, \quad A_4, \quad A_6, \quad A_8$$

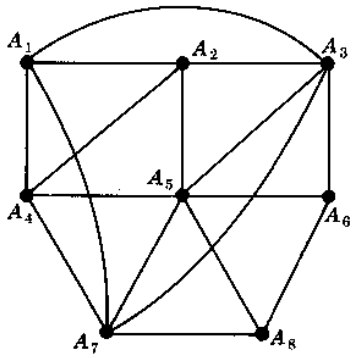


Fig. 8-23

The first color is assigned to vertices A_5 and A_1. The second color is assigned to vertices A_3, A_4, and A_8. The third color is assigned to vertices A_7, A_2, and A_6. All the vertices have been assigned a color, and so G is

3-colorable. Observe that G is not 2-colorable since vertices A_1, A_2, and A_3, which are connected to each other, must be assigned different colors. Accordingly, $\chi(G) = 3$.

(*b*) Consider the complete graph K_n with n vertices. Since every vertex is adjacent to every other vertex, K_n requires n colors in any coloring. Thus $\chi(K_n) = n$.

There is no simple way to actually determine whether an arbitrary graph is n-colorable. However, the following theorem (proved in Problem 8.22) gives a simple characterization of 2-colorable graphs.

Theorem 8.11: The following are equivalent for a graph G:
(i) G is 2-colorable.
(ii) G is bipartite.
(iii) Every cycle of G has even length.

There is no limit on the number of colors that may be required for a coloring of an arbitrary graph since, for example, the complete graph K_n requires n colors. However, if we restrict ourselves to planar graphs, regardless of the number of vertices, five colors suffice. Specifically, in Problem 8.24 we prove:

Theorem 8.12: Any planar graph is 5-colorable.

Actually, since the 1850s mathematicians have conjectured that planar graphs are 4-colorable since every known planar graph is 4-colorable. Kenneth Appel and Wolfgang Haken finally proved this conjecture to be true in 1976. That is:

Four Color Theorem (Appel and Haken): Any planar graph is 4-colorable.

We discuss this theorem in the next subsection.

Dual Maps and the Four Color Theorem

Consider a map M, say the map M in Fig. 8-24(*a*). In other words, M is a planar representation of a planar multigraph. Two regions of M are said to be *adjacent* if they have an edge in common. Thus the regions r_2 and r_5 in Fig. 8-24(*a*) are adjacent, but the regions r_3 and r_5 are not. By a *coloring* of M we mean an assignment of a color to each region of M such that adjacent regions have different colors. A map M is *n-colorable* if there exists a coloring of M which uses n colors. Thus the map M in Fig. 8-24(*a*) is 3-colorable since the regions can be assigned the following colors:

r_1 red, r_2 white, r_3 red, r_4 white, r_5 red, r_6 blue

Observe the similarity between this discussion on coloring maps and the previous discussion on coloring graphs. In fact, using the concept of the dual map defined below, the coloring of a map can be shown to be equivalent to the vertex coloring of a planar graph.

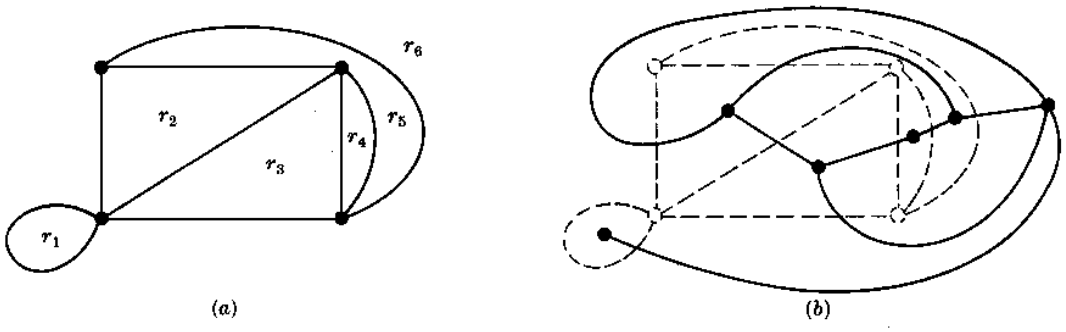


Fig. 8-24

Consider a map M. In each region of M we choose a point, and if two regions have an edge in common then we connect the corresponding points with a curve through the common edge. These curves can be drawn so that they are noncrossing. Thus we obtain a new map M^*, called the *dual* of M, such that each vertex of M^* corresponds to exactly one region of M. Figure 8-24(b) shows the dual of the map of Fig. 8-24(a). One can prove that each region of M^* will contain exactly one vertex of M and that each edge of M^* will intersect exactly one edge of M and vice versa. Thus M will be the dual of the map M^*.

Observe that any coloring of the regions of a map M will correspond to a coloring of the vertices of the dual map M^*. Thus M is n-colorable if and only if the planar graph of the dual map M^* is vertex n-colorable. Thus the above theorem can be restated as follows:

Four Color Theorem (Appel and Haken): If the regions of any map M are colored so that adjacent regions have different colors, then no more than four colors are required.

The proof of the above theorem uses computers in an essential way. Specifically, Appel and Haken first showed that if the four color theorem was false, then there must be a counterexample among one of approximately 2000 different types of planar graphs. They then showed, using the computer, that none of these types of graphs has such a counterexample. The examination of each different type of graph seems to be beyond the grasp of human beings without the use of a computer. Thus the proof, unlike most proofs in mathematics, is technology dependent; that is, it depended on the development of high-speed computers.

8.11 REPRESENTING GRAPHS IN COMPUTER MEMORY

There are two standard ways of maintaining a graph G in the memory of a computer. One way, called the *sequential representation* of G, is by means of its adjacency matrix A. The other way, called the *linked representation* or *adjacency structure* of G, uses linked lists of neighbors. Matrices are usually used when the graph G is dense, and linked lists are usually used when G is sparse. (A graph G with m vertices and n edges is said to be *dense* when $m = O(n^2)$ and *sparse* when $m = O(n)$ or even $O(n \log n)$.)

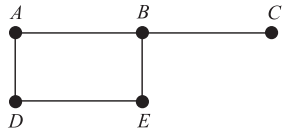
Regardless of the way one maintains a graph G in memory, the graph G is normally input into the computer by its formal definition, that is, as a collection of vertices and a collection of pairs of vertices (edges).

Adjacency Matrix

Suppose G is a graph with m vertices, and suppose the vertices have been ordered, say, $v_1, v_2, \ldots, v_m$. Then the *adjacency matrix* $A = [a_{ij}]$ of the graph G is the $m \times m$ matrix defined by

$$a_{ij} = \begin{cases} 1 & \text{if } v_i \text{ is adjacent to } v_j \\ 0 & \text{otherwise} \end{cases}$$

Figure 8-25(b) contains the adjacency matrix of the graph G in Fig. 8-25(a) where the vertices are ordered A, B, C, D, E. Observe that each edge $\{v_i, v_j\}$ of G is represented twice, by $a_{ij} = 1$ and $a_{ji} = 1$. Thus, in particular, the adjacency matrix is symmetric.



(a)

	A	B	C	D	E
A	0	1	0	1	0
B	1	0	1	0	1
C	0	1	0	0	0
D	1	0	0	0	1
E	0	1	0	1	0

(b)

Fig. 8-25

The adjacency matrix A of a graph G does depend on the ordering of the vertices of G, that is, a different ordering of the vertices yields a different adjacency matrix. However, any two such adjacency matrices are closely related in that one can be obtained from the other by simply interchanging rows and columns. On the other hand, the adjacency matrix does not depend on the order in which the edges (pairs of vertices) are input into the computer.

There are variations of the above representation. If G is a multigraph, then we usually let a_{ij} denote the number of edges $\{v_i, v_j\}$. Moreover, if G is a weighted graph, then we may let a_{ij} denote the weight of the edge $\{v_i, v_j\}$.

Linked Representation of a Graph *G*

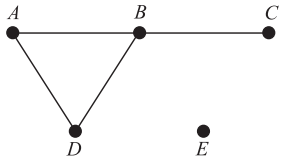
Let G be a graph with m vertices. The representation of G in memory by its adjacency matrix A has a number of major drawbacks. First of all it may be difficult to insert or delete vertices in G. The reason is that the size of A may need to be changed and the vertices may need to be reordered, so there may be many, many changes in the matrix A. Furthermore, suppose the number of edges is $O(m)$ or even $O(m \log m)$, that is, suppose G is sparse. Then the matrix A will contain many zeros; hence a great deal of memory space will be wasted. Accordingly, when G is sparse, G is usually represented in memory by some type of *linked representation*, also called an *adjacency structure*, which is described below by means of an example.

Consider the graph G in Fig. 8-26(a). Observe that G may be equivalently defined by the table in Fig. 8-26(b) which shows each vertex in G followed by its *adjacency list*, i.e., its list of adjacent vertices (*neighbors*). Here the symbol $\varnothing$ denotes an empty list. This table may also be presented in the compact form

$$G = [A: B, D; \quad B: A, C, D; \quad C: B; \quad D: A, B; \quad E: \varnothing]$$

where a colon ":" separates a vertex from its list of neighbors, and a semicolon ";" separates the different lists.

Remark: Observe that each edge of a graph G is represented twice in an adjacency structure; that is, any edge, say $\{A, B\}$, is represented by B in the adjacency list of A, and also by A in the adjacency list of B. The graph G in Fig. 8-26(a) has four edges, and so there must be 8 vertices in the adjacency lists. On the other hand, each vertex in an adjacency list corresponds to a unique edge in the graph G.



(a)

Vertex	Adjacency list
A	B, D
B	A, C, D
C	B
D	A, B
E	$\varnothing$

(b)

Fig. 8-26

The *linked representation* of a graph G, which maintains G in memory by using its adjacency lists, will normally contain two files (or sets of records), one called the Vertex File and the other called the Edge File, as follows.

(a) ***Vertex File***: The Vertex File will contain the list of vertices of the graph G usually maintained by an array or by a linked list. Each record of the Vertex File will have the form

VERTEX	NEXT-V	PTR	

Here VERTEX will be the name of the vertex, NEXT-V points to the next vertex in the list of vertices in the Vertex File when the vertices are maintained by a linked list, and PTR will point to the first element in the adjacency list of the vertex appearing in the Edge File. The shaded area indicates that there may be other information in the record corresponding to the vertex.

(*b*) ***Edge File***: The Edge File contains the edges of the graph G. Specifically, the Edge File will contain all the adjacency lists of G where each list is maintained in memory by a linked list. Each record of the Edge File will correspond to a vertex in an adjacency list and hence, indirectly, to an edge of G. The record will usually have the form

EDGE	ADJ	NEXT	

Here:

(1) EDGE will be the name of the edge (if it has one).
(2) ADJ points to the location of the vertex in the Vertex File.
(3) NEXT points to the location of the next vertex in the adjacency list.

We emphasize that each edge is represented twice in the Edge File, but each record of the file corresponds to a unique edge. The shaded area indicates that there may be other information in the record corresponding to the edge.

Figure 8-27 shows how the graph G in Fig. 8-26(*a*) may appear in memory. Here the vertices of G are maintained in memory by a linked list using the variable START to point to the first vertex. (Alternatively, one could use a linear array for the list of vertices, and then NEXT-V would not be required.) Note that the field EDGE is not needed here since the edges have no name. Figure 8-27 also shows, with the arrows, the adjacency list $[D, C, A]$ of the vertex B.

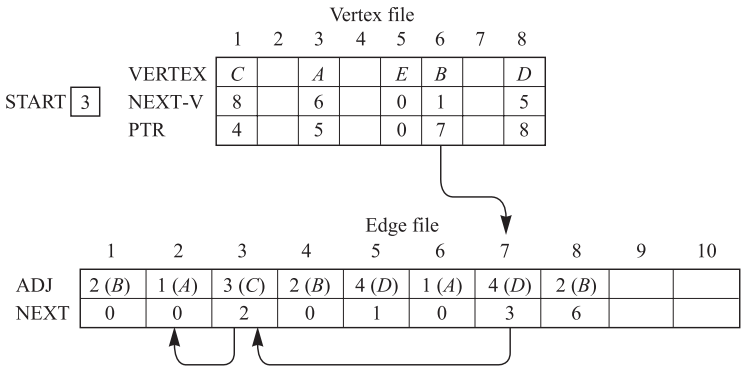
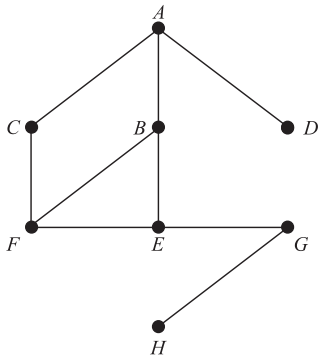

Vertex file
1 2 3 4 5 6 7 8
VERTEX C A E B D
START 3
NEXT-V 8 6 0 1 5
PTR 4 5 0 7 8
Edge file
1 2 3 4 5 6 7 8 9 10
ADJ 2 (B) 1 (A) 3 (C) 2 (B) 4 (D) 1 (A) 4 (D) 2 (B)
NEXT 0 0 2 0 1 0 3 6

Fig. 8-27

8.12 GRAPH ALGORITHMS

This section discusses two important graph algorithms which systematically examine the vertices and edges of a graph G. One is called a *depth-first search* (DFS) and the other is called a *breadth-first search* (BFS). Other graph algorithms will be discussed in the next chapter in connection with directed graphs. Any particular graph algorithm may depend on the way G is maintained in memory. Here we assume G is maintained in memory by its adjacency structure. Our test graph G with its adjacency structure appears in Fig. 8-28.



(*a*)

Vertex	Adjacency list
A	*B*, *C*, *D*
B	*A*, *E*, *F*
C	*A*, *F*
D	*A*
E	*B*, *F*, *G*
F	*B*, *C*, *E*
G	*E*, *H*
H	*G*

(*b*)

Fig. 8-28

During the execution of our algorithms, each vertex (node) N of G will be in one of three states, called the *status* of N, as follows:

STATUS = 1: (Ready state) The initial state of the vertex N.
STATUS = 2: (Waiting state) The vertex N is on a (waiting) list, waiting to be processed.
STATUS = 3: (Processed state) The vertex N has been processed.

The waiting list for the depth-first search will be a (modified) STACK, whereas the waiting list for the breadth-first search will be a QUEUE.

Depth-first Search

The general idea behind a depth-first search beginning at a starting vertex A is as follows. First we process the starting vertex A. Then we process each vertex N along with a path P which begins at A; that is, we process a neighbor of A, then a neighbor of a neighbor of A, and so on. After coming to a "dead end", that is, to a vertex with no unprocessed neighbor, we backtrack on the path P until we can continue along another path P'. And so on. The backtracking is accomplished by using a STACK to hold the initial vertices of future possible paths. We also need a field STATUS which tells us the current status of any vertex so that no vertex is processed more than once. The algorithm follows.

Algorithm 8.12A (Depth-first Search): This algorithm executes a depth-first search on a graph G beginning with a starting vertex A.

Step 1. Initialize all vertices to the ready state (STATUS = 1).

Step 2. Push the starting vertex A onto STACK and change the status of A to the waiting state (STATUS = 2).

Step 3. Repeat Steps 4 and 5 until STACK is empty.

Step 4. Pop the top vertex N of STACK. Process N, and set STATUS $(N) = 3$, the processed state.

Step 5. Examine each neighbor J of N.

(a) If STATUS $(J) = 1$ (ready state), push J onto STACK and reset STATUS $(J) = 2$ (waiting state).
(b) If STATUS $(J) = 2$ (waiting state), delete the previous J from the STACK and push the current J onto STACK.
(c) If STATUS $(J) = 3$ (processed state), ignore the vertex J.
[End of Step 3 loop.]

Step 6. Exit.

The above algorithm will process only those vertices which are connected to the starting vertex A, that is, the connected component including A. Suppose one wants to process all the vertices in the graph G. Then the algorithm must be modified so that it begins again with another vertex (which we call B) that is still in the ready state (STATE = 1). This vertex B can be obtained by traversing through the list of vertices.

Remark: The structure STACK in the above algorithm is not technically a stack since, in Step 5(b), we allow a vertex J to be deleted and then inserted in the front of the stack. (Although it is the same vertex J, it usually represents a different edge in the adjacency structure.) If we do not move J in Step 5(b), then we obtain an alternate form of DFS.

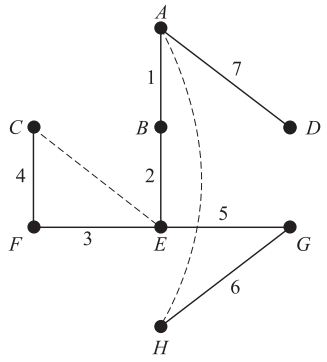
EXAMPLE 8.4 Suppose the DFS Algorithm 8.12A is applied to the graph in Fig. 8-28. The vertices are processed in the following order:

$$A, \quad B, \quad E, \quad F, \quad C, \quad G, \quad H, \quad D$$

Specifically, Fig. 8-29(a) shows the sequence of waiting lists in STACK and the vertices being processed. We have used the slash / to indicate that a vertex is deleted from the waiting list. Each vertex, excluding A, comes from an adjacency list and hence corresponds to an edge of the graph. These edges form a spanning tree of G which is pictured in Fig. 8-29(b). The numbers indicate the order that the edges are added to the tree, and the dashed lines indicate backtracking.

Vertex	STACK
	A
A	B, C, D
B	E, F, C, D
E	$F, G, \not{F}, C, D$
F	$C, G, \not{C}, D$
C	G, D
G	H, D
H	D
D	

(a)



(b)

Fig. 8-29

Breadth-first Search

The general idea behind a breadth-first search beginning at a starting vertex A is as follows. First we process the starting vertex A. Then we process all the neighbors of A. Then we process all the neighbors of neighbors of A. And so on. Naturally we need to keep track of the neighbors of a vertex, and we need to guarantee that no vertex is processed twice. This is accomplished by using a QUEUE to hold vertices that are waiting to be processed, and by a field STATUS which tells us the current status of a vertex. The algorithm follows.

Algorithm 8.12B (Breadth-first Search): This algorithm executes a breadth-first search on a graph G beginning with a starting vertex A.

Step 1. Initialize all vertices to the ready state (STATUS = 1).

Step 2. Put the starting vertex A in QUEUE and change the status of A to the waiting state (STATUS = 2).

Step 3. Repeat Steps 4 and 5 until QUEUE is empty.

Step 4. Remove the front vertex N of QUEUE. Process N, and set STATUS $(N) = 3$, the processed state.

Step 5. Examine each neighbor J of N.
(a) If STATUS $(J) = 1$ (ready state), add J to the rear of QUEUE and reset STATUS $(J) = 2$ (waiting state).
(b) If STATUS $(J) = 2$ (waiting state) or STATUS $(J) = 3$ (processed state), ignore the vertex J.
[End of Step 3 loop.]

Step 6. Exit.

Again, the above algorithm will process only those vertices which are connected to the starting vertex A, that is, the connected component including A. Suppose one wants to process all the vertices in the graph G. Then the algorithm must be modified so that it begins again with another vertex (which we call B) that is still in the ready state (STATUS = 1). This vertex B can be obtained by traversing through the list of vertices.

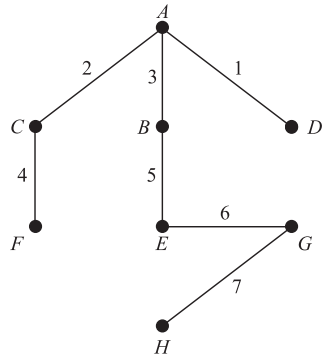
EXAMPLE 8.5 Suppose the BFS Algorithm 8.12B is applied to the graph in Fig. 8-28. The vertices are processed in the following order:

$$A, \quad D, \quad C, \quad B, \quad F, \quad E, \quad G, \quad H$$

Specifically, Fig. 8-30(a) shows the sequence of waiting lists in QUEUE and the vertices being processed. Again, each vertex, excluding A, comes from an adjacency list and hence corresponds to an edge of the graph. These edges form a spanning tree of G which is pictured in Fig. 8-30(b). Again, the numbers indicate the order the edges are added to the tree. Observe that this spanning tree is different than the one in Fig. 8-29(b) which came from a depth-first search.

Vertex	QUEUE
	A
A	B, C, D
D	B, C
C	$F, B,$
B	E, F
F	E
E	G
G	H
H	

(a)



(b)

Fig. 8-30

Solved Problems

GRAPH TERMINOLOGY

8.1. Consider Fig. 8-31. (*a*) Describe formally the graph G in the diagram, that is, find the set $V(G)$ of vertices of G and the set $E(G)$ of edges of G. (*b*) Find the degree of each vertex and verify Theorem 8.1 for this graph.

(*a*) There are five vertices so $V(G) = \{A, B, C, D, E\}$. There are seven pairs $\{x, y\}$ of vertices where the vertex x is connected with the vertex y; hence

$$E(G) = [\{A, B\}, \{A, C\}, \{A, D\}, \{B, C\}, \{B, E\}, \{C, D\}, \{C, E\}]$$

(*b*) The degree of a vertex is equal to the number of edges to which it belongs; e.g., deg $(A) = 3$ since A belongs to the three edges $\{A, B\}, \{A, C\}, \{A, D\}$. Similarly,

$$\deg(B) = 3,\ \deg(C) = 4,\ \deg(D) = 2,\ \deg(E) = 2$$

The sum of the degrees of the vertices is

$$3 + 3 + 4 + 2 + 2 = 14$$

which does equal twice the number of edges.

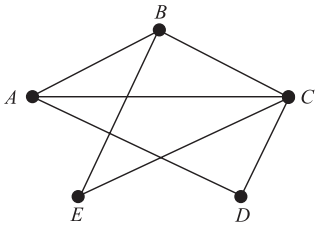


Fig. 8-31

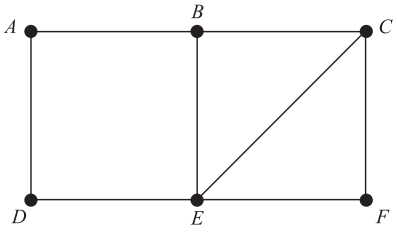


Fig. 8-32

8.2. Consider the graph G in Fig. 8-32. Find: (*a*) all simple paths from A to F; (*b*) all trails from A to F; (*c*) $d(A, F)$; the distance from A to F; (*d*) diam(G), the diameter of G; (*e*) all cycles which include vertex A; (*f*) all cycles in G.

(*a*) A simple path from A to F is a path such that no vertex, and hence no edge, is repeated. There are seven such paths, four beginning with the edges $\{A, B\}$ and three beginning with the ege $\{A, D\}$:

$$(A, B, C, F), \quad (A, B, C, E, F), \quad (A, B, E, F), \quad (A, B, E, C, F);$$
$$(A, D, E, F), \quad (A, D, E, B, C, F), \quad (A, D, E, C, F)$$

(*b*) A trail from A to F is a path such that no edge is repeated. There are nine such trails, the seven simple paths from (*a*) together with

$$(A, D, E, B, C, E, F) \qquad \text{and} \qquad (A, D, E, C, B, E, F)$$

(*c*) There is a path, e.g., (A, B, C, F), from A to F of length 3 and no shorter path from A to F; hence $d(A, F) = 3$.

(*d*) The distance between any two vertices is not greater than 3, and the distance from A to F is 3; hence diam $(G) = 3$.

(*e*) A cycle is a closed path in which no vertex is repeated (except the first and last). There are three cycles which include vertex A:

$$(A, B, E, D), \quad (A, B, C, E, D, A), \quad (A, B, C, F, E, D, A)$$

(*f*) There are six cycles in G; the three in (*e*) and

$$(B, C, E, B), \quad (C, F, E, C), \quad (B, C, F, E, B)$$

8.3. Consider the multigraphs G in Fig. 8-33. (a) Which of them are connected? If a graph is not connected, find its connected components. (b) Which are cycle-free (without cycles)? (c) Which are loop-free (without loops)? (d) Which are graphs?

(a) Only (1) and (3) are connected. (2) is disconnected; its connected components are $\{A, D, E\}$ and $\{B, C\}$. (4) is disconnected; its connected components are $\{A, B, E\}$ and $\{C, D\}$.

(b) Only (1) and (4) are cycle-free. (2) has the cycle (A, D, E, A), and (3) has the cycle (A, B, E, A)

(c) Only (4) has a loop which is $\{B, B\}$.

(d) Only (1) and (2) are graphs. Multigraph (3) has multiple edges $\{A, E\}$ and $\{A, E\}$; and (4) has both multiple edges $\{C, D\}$ and $\{C, D\}$ and a loop $\{B, B\}$.

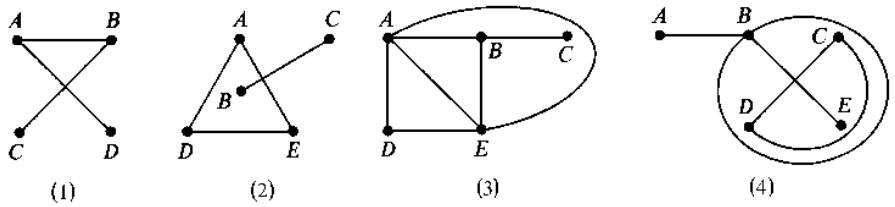


Fig. 8-33

8.4. Let G be the graph in Fig. 8-34(a). Find: (a) all simple paths from A to C; (b) all cycles; (c) subgraph H of G generated by $V' = \{B, C, X, Y\}$; (d) $G - Y$; (e) all cut points; (f) all bridges.

(a) There are two simple paths from A to C: (A, X, Y, C) and (A, X, B, Y, C).

(b) There is only one cycle: (B, X, Y, B).

(c) As pictured in Fig. 8-34(b), H consists of the vertices V' and the set E' of all edges whose end points belong to V', that is,

$$E' = [\{B, X\}, \{X, Y\}, \{B, Y\}, \{C, Y\}]$$

(d) Delete vertex Y from G and all edges which contain Y to obtain the graph $G - Y$ in Fig. 8-34(c). (Note Y is a cutpoint since $G - Y$ is disconnected.)

(e) Vertices A, X, and Y are cut points.

(f) An edge e is a bridge if $G - e$ is disconnected. Thus there are three bridges: $\{A, Z\}$, $\{A, X\}$, and $\{C, Y\}$.

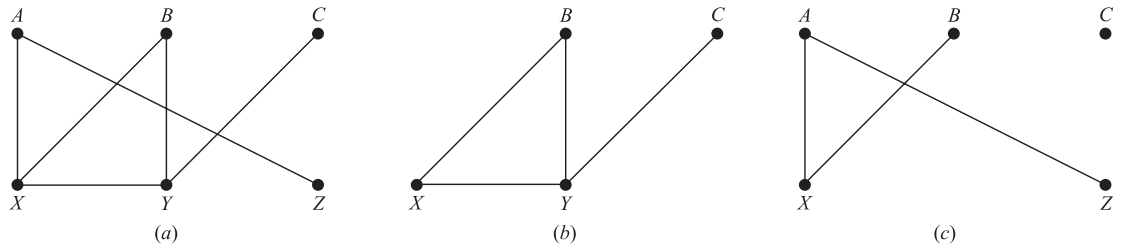


Fig. 8-34

8.5. Consider the graph G in Fig. 8-32. Find the subgraphs obtained when each vertex is deleted. Does G have any cut points?

When we delete a vertex from G, we also have to delete all edges which contain the vertex. The six graphs obtained by deleting each of the vertices of G are shown in Fig. 8-35. All six graphs are connected; hence no vertex is a cut prints.

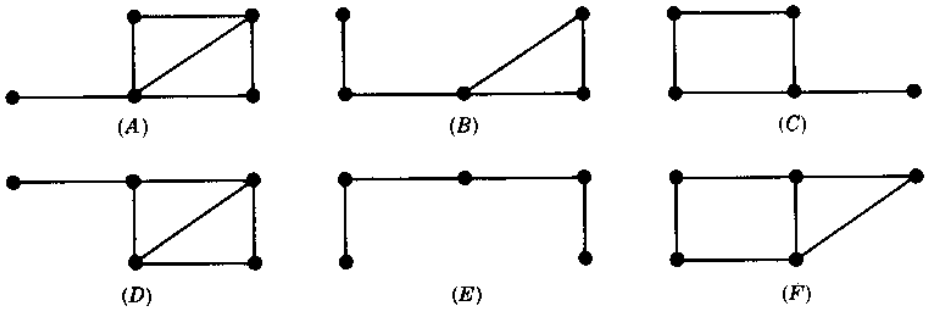


Fig. 8-35

8.6. Show that the six graphs obtained in Problem 8.5 are distinct, that is, no two of them are isomorphic. Also show that (B) and (C) are homeomorphic.

The degrees of the five vertices of any graph cannot be paired off with the degrees of any other graph, except for (B) and (C). Hence none of the graphs is isomorphic except possibly (B) and (C).

However, if we delete the vertex of degree 3 in (B) and (C), we obtain distinct subgraphs. Thus (B) and (C) are also nonisomorphic; hence all six graphs are distinct. However, (B) and (C) are homeomorphic since they can be obtained, respectively, from the isomorphic graphs in Fig. 8-36 by adding appropriate vertices.

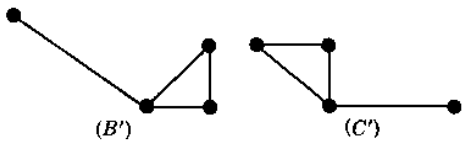


Fig. 8-36

TRAVERSABLE GRAPHS, EULER AND HAMILTONIAN CIRCUITS

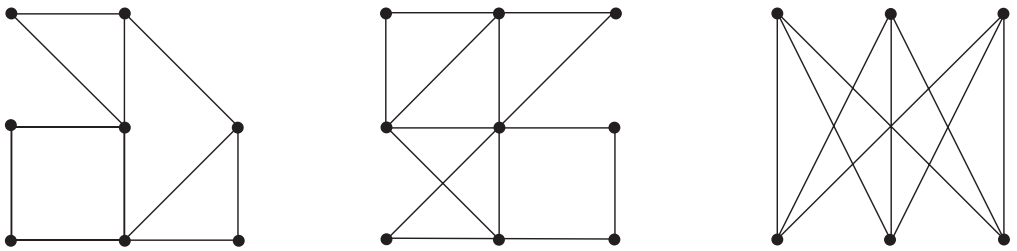
8.7. Consider each graph G in Fig. 8-37. Which of them are traversable, that is, have Euler paths? Which are Eulerian, that is, have an Euler circuit? For those that do not, explain why.

G is traversable (has an Euler path) if only 0 or 2 vertices have odd degree, and G is Eulerian (has an Euler circuit) if all vertices are of even degree (Theorem 8.3).

(*a*) Traversable, since there are two odd vertices. The traversable path must begin at one of the odd vertices and will end at the other.

(*b*) Traversable, since all vertices are even. Thus G has an Euler circuit.

(*c*) Since six vertices have odd degrees, G is not traversable.



(*a*) (*b*) (*c*)

Fig. 8-37

8.8. Which of the graphs G in Fig. 8-37 have a Hamiltonian circuit? If not, why not?

Graphs (*a*) and (*c*) have Hamiltonian circuits. (The reader should be able to easily find one of them.) However, graph (*b*) has no Hamiltonian circuit. For if α is a Hamiltonian circuit, then α must connect the middle vertex with the lower right vertex, then proceed along the bottom row to the lower right vertex, then vertically to the middle right, but then is forced back to the central vertex before visiting the remaining vertices.

8.9. Prove Theorem 8.3 (Euler): A finite connected graph G is Eulerian if and only if each vertex has even degree.

Suppose G is Eulerian and T is a closed Eulerian trail. For any vertex v of G, the trail T enters and leaves v the same number of times without repeating any edge. Hence v has even degree.

Suppose conversely that each vertex of G has even degree. We construct an Eulerian trail. We begin a trail T_1 at any edge e. We extend T_1 by adding one edge after the other. If T_1 is not closed at any step, say, T_1 begins at u but ends at $v \neq u$, then only an odd number of the edges incident on v appear in T_1; hence we can extend T_1 by another edge incident on v. Thus we can continue to extend T_1 until T_1 returns to its initial vertex u, i.e., until T_1 is closed. If T_1 includes all the edges of G, then T_1 is our Eulerian trail.

Suppose T_1 does not include all edges of G. Consider the graph H obtained by deleting all edges of T_1 from G. H may not be connected, but each vertex of H has even degree since T_1 contains an even number of the edges incident on any vertex. Since G is connected, there is an edge e' of H which has an endpoint u' in T_1. We construct a trail T_2 in H beginning at u' and using e'. Since all vertices in H have even degree, we can continue to extend T_2 in H until T_2 returns to u' as pictured in Fig. 8-38. We can clearly put T_1 and T_2 together to form a larger closed trail in G. We continue this process until all the edges of G are used. We finally obtain an Eulerian trail, and so G is Eulerian.

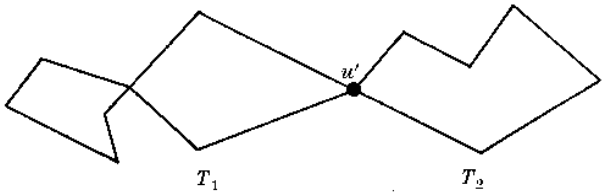


Fig. 8-38

SPECIAL GRAPHS

8.10. Draw the graph $K_{2,5}$.

$K_{2,5}$ consists of seven vertices partitioned into a set M of 2 vertices, say, u_1 and u_2, and a set N of 5 vertices, say, $v_1, v_2, \ldots, v_5$, and all possible edges from a vertex u_i to a vertex v_j. Thus there are 10 edges. The graph appears in Fig. 8-39.

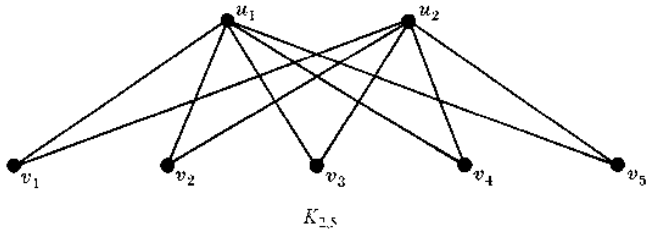


Fig. 8-39

8.11. Which connected graphs can be both regular and bipartite?

The bipartite graph $K_{m,m}$ is regular of degree m since each vertex is connected to m other vertices and hence its degree is m. Subgraphs of $K_{m,m}$ can also be regular if m disjoint edges are deleted. For example, the subgraph of $K_{4,4}$ shown in Fig. 8-40 is 3-regular. We can continue to delete m disjoint edges and each time obtain a regular graph of one less degree. These graphs may be disconnected, but in any case their connected components have the desired properties.

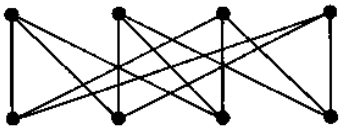


Fig. 8-40

TREES, SPANNING TREES

8.12. Draw all trees with exactly six vertices.

There are six such trees which are exhibited in Fig. 8-41. The first tree has diameter 5, the next two diameter 4, the next two diameter 3, and the last one diameter 2. Any other tree with 6 nodes is isormorphic to one of these trees.

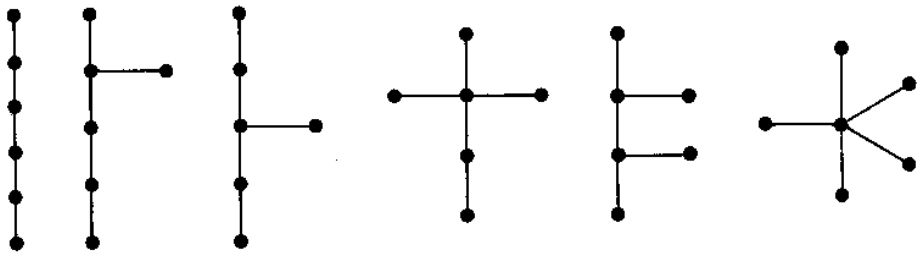


Fig. 8-41

8.13. Find all spanning trees of the graph G shown in Fig. 8-42(a).

There are eight such spanning trees as shown in Fig. 8-42(b). Each spanning tree must have $4 - 1 = 3$ edges since G has four vertices. Thus each tree can be obtained by deleting two of the five edges of G. This can be done in 10 ways, except that two of the ways lead to disconnected graphs. Hence the above eight spanning trees are all the spanning trees of G.

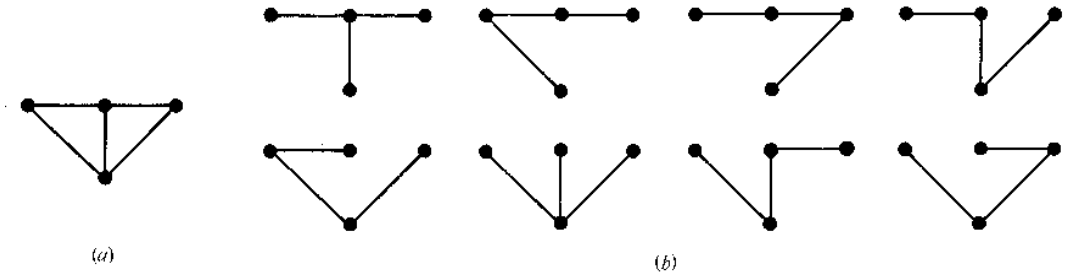


Fig. 8-42

8.14. Find a minimal spanning tree T for the weighted graph G in Fig. 8-43(a).

Since G has $n = 9$ vertices, T must have $n - 1 = 8$ edges. Apply Algorithm 8.8A, that is, keep deleting edges with maximum length and without disconnecting the graph until only $n - 1 = 8$ edges remain. Alternatively, apply Algorithm 8.8B, that is, beginning with the nine vertices, keep adding edges with minimum length and without forming any circle until $n - 1 = 8$ edges are added. Both methods give a minimum spanning tree such as that shown in Fig. 8-43(b).

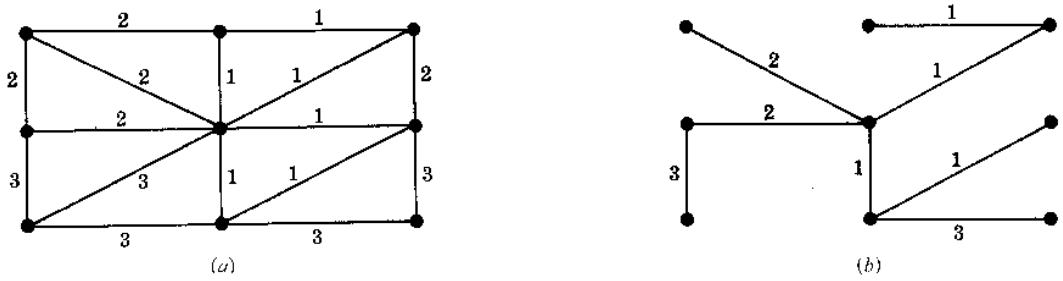


Fig. 8-43

8.15. Let G be a graph with more than one vertex. Prove the following are equivalent: (i) G is a tree. (ii) Each pair of vertices is connected by exactly one simple path. (iii) G is connected; but $G - e$ is disconnected for any edge e of G. (iv) G is cycle-free, but if any edge is added to G then the resulting graph has exactly one cycle.

(i) implies (ii). Let u and v be two vertices in G. Since G is a tree, G is connected so there is at least one path between u and v. By Problem 8.37 there can only be one simple path between u and v, otherwise G will contain a cycle.

(ii) implies (iii). Suppose we delete an edge $e = \{u, v\}$ from G. Note e is a path from u to v. Suppose the resulting graph $G - e$ has a path P from u to v. Then P and e are two distinct paths from u to v, which contradicts the hypothesis. Thus there is no path between u and v in $G - e$, so $G - e$ is disconnected.

(iii) implies (iv). Suppose G contains a cycle C which contains an edge $e = \{u, v\}$. By hypothesis, G is connected but $G' = G - e$ is disconnected, with u and v belonging to different components of G' (Problem

8.41). This contradicts the fact that u and v are connected by the path $P = C - e$ which lies in G'. Hence G is cycle-free. Now let x and y be vertices of G and let H be the graph obtained by adjoining the edge $e = \{x, y\}$ to G. Since G is connected, there is a path P from x to y in G; hence $C = Pe$ forms a cycle in H. Suppose H contains another cycle C'. Since G is cycle-free, C' must contain the edge e, say $C' = P'e$. Then P and P' are two simple paths in G from x to y. (See Fig. 8-44.) By Problem 8.37, G contains a cycle, which contradicts the fact that G is cycle-free. Hence H contains only one cycle.

(iv) implies (i). Since adding any edge $e = \{x, y\}$ to G produces a cycle, the vertices x and y must already be connected in G. Hence G is connected and by hypothesis G is cycle-free; that is, G is a tree.

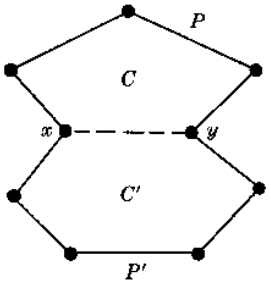


Fig. 8-44

8.16. Prove Theorem 8.6: Let G be a finite graph with $n \geq 1$ vertices. Then the following are equivalent. (i) G is a tree. (ii) G is a cycle-free and has $n - 1$ edges. (iii) G is connected and has $n - 1$ edges.

The proof is by induction on n. The theorem is certainly true for the graph with only one vertex and hence no edges. That is, the theorem holds for $n = 1$. We now assume that $n > 1$ and that the theorem holds for graphs with less than n vertices.

(i) implies (ii). Suppose G is a tree. Then G is cycle-free, so we only need to show that G has $n - 1$ edges. By Problem 8.38, G has a vertex of degree 1. Deleting this vertex and its edge, we obtain a tree T which has $n - 1$ vertices. The theorem holds for T, so T has $n - 2$ edges. Hence G has $n - 1$ edges.

(ii) implies (iii). Suppose G is cycle-free and has $n - 1$ edges. We only need show that G is connected. Suppose G is disconnected and has k components, $T_1, \ldots, T_k$, which are trees since each is connected and cycle-free. Say T_i has n_i vertices. Note $n_i < n$. Hence the theorem holds for T_i, so T_i has $n_i - 1$ edges. Thus

$$n = n_1 + n_2 + \cdots + n_k$$

and

$$n - 1 = (n_1 - 1) + (n_2 - 1) + \cdots + (n_k - 1) = n_1 + n_2 + \cdots + n_k - k = n - k$$

Hence $k = 1$. But this contradicts the assumption that G is disconnected and has $k > 1$ components. Hence G is connected.

(iii) implies (i). Suppose G is connected and has $n - 1$ edges. We only need to show that G is cycle-free. Suppose G has a cycle containing an edge e. Deleting e we obtain the graph $H = G - e$ which is also connected. But H has n vertices and $n - 2$ edges, and this contradicts Problem 8.39. Thus G is cycle-free and hence is a tree.

PLANAR GRAPHS

8.17. Draw a planar representation of each graph in Fig. 8-45, if possible.

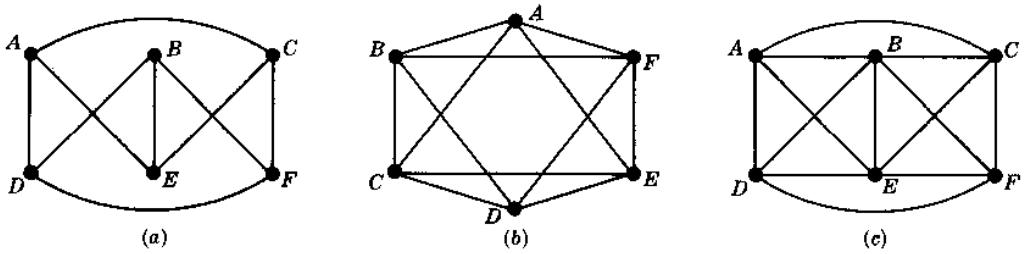


Fig. 8-45

(*a*) Redrawing the positions of the vertices B and E, we get a planar representation of the graph, as in Fig. 8-46(*a*).

(*b*) This is not the star graph K_5. This has a planar representation as in Fig. 8-46(*b*).

(*c*) This graph is nonplanar. The utility graph $K_{3,3}$ is a subgraph, as shown in Fig. 8-46(*c*), where we have redrawn the positions of C and F.

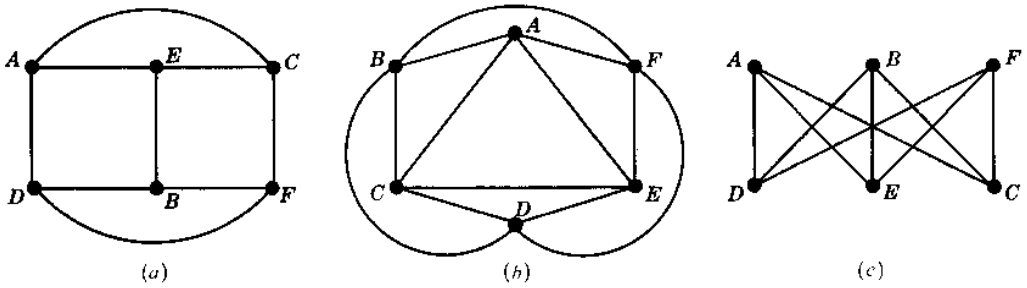


Fig. 8-46

8.18. Count the number V of vertices, the number E of edges and the number R of regions of each map in Fig. 8-47 and verify Euler's formula. Also find the degree of the outside region.

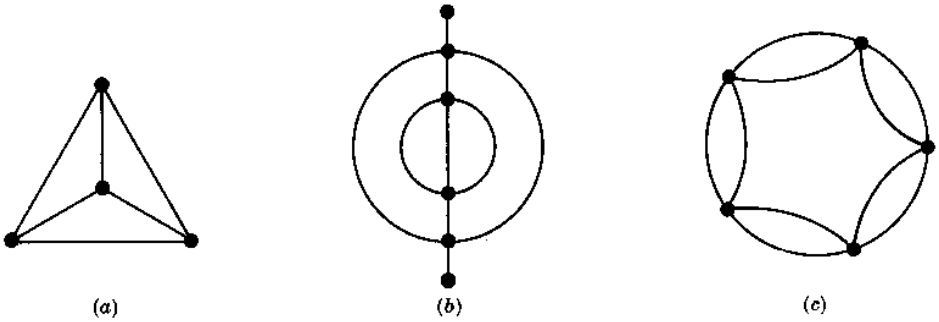


Fig. 8-47

(*a*) $V = 4$, $E = 6$, $R = 4$. Hence $V - E + R = 4 - 6 + 4 = 2$. Also $d = 3$.

(*b*) $V = 6$, $E = 9$, $R = 5$; so $V - E + R = 6 - 9 + 5 = 2$. Here $d = 6$ since two edges are counted twice.

(*c*) $V = 5$, $E = 10$, $R = 7$. Hence $V - E + R = 5 - 10 + 7 = 2$. Here $d = 5$.

8.19. Find the minimum number n of colors required to paint each map in Fig. 8-47.

(*a*) $n = 4$; (*b*) $n = 3$; (*c*) only two colors are needed, i.e., $n = 2$.

8.20. Prove Theorem 8.8 (Euler): $V - E + R = 2$.

Suppose the connected map M consists of a single vertex P as in Fig. 8-48(*a*). Then $V = 1, E = 0$, and $R = 1$. Hence $V - E + R = 2$. Otherwise M can be built up from a single vertex by the following two constructions:

(1) Add a new vertex Q_2 and connect it to an existing vertex Q_1 by an edge which does not cross any existing edge as in Fig. 8-48(*b*).

(2) Connect two existing vertices Q_1 and Q_2 by an edge e which does not cross any existing edge as in Fig. 8-48(*c*).

Neither operation changes the value of $V - E + R$. Hence M has the same value of $V - E + R$ as the map consisting of a single vertex, that is, $V - E + R = 2$. Thus the theorem is proved.

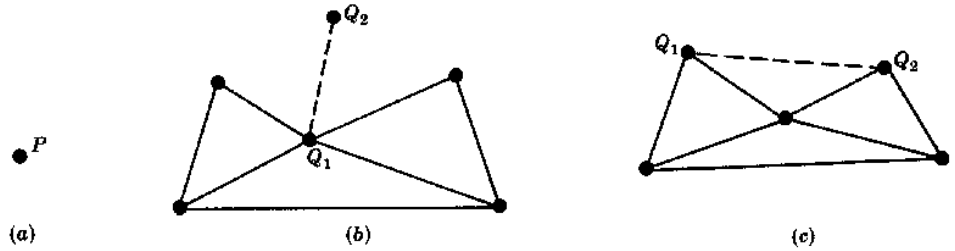


Fig. 8-48

8.21. Use the Welch-Powell algorithm to paint the graph in Fig. 8-49, and find the chromatic number n of the graph.

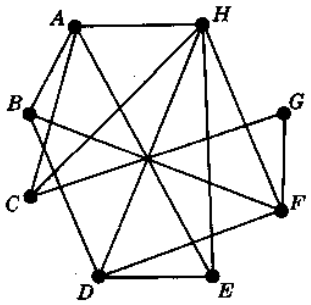


Fig. 8-49

First order the vertices according to decreasing degrees to obtain the sequence

$$H, \quad A, \quad D, \quad F, \quad B, \quad C, \quad E, \quad G$$

Proceeding sequentially, we use the first color to paint the vertices H, B, and then G. (We cannot paint A, D, or F the first color since each is connected to H, and we cannot paint C or E the first color since each is connected to either H or B.) Proceeding sequentially with the unpainted vertices, we use the second color to paint the vertices A and D. The remaining vertices F, C, and E can be painted with the third color. Thus the chromatic number n cannot be greater than 3. However, in any coloring, H, D, and E must be painted different colors since they are connected to each other. Hence $n = 3$.

8.22. Prove Theorem 8.11: The following are equivalent for a graph G: (i) G is 2-colorable. (ii) G is bipartite. (iii) Every cycle of G has even length.

(i) implies (ii). Suppose G is 2-colorable. Let M be the set of vertices painted the first color, and let N be the set of vertices painted the second color. Then M and N form a bipartite partition of the vertices of G since neither the vertices of M nor the vertices of N can be adjacent to each other since they are of the same color.

(ii) implies (iii). Suppose G is bipartite and M and N form a bipartite partition of the vertices of G. If a cycle begins at a vertex u of, say, M, then it will go to a vertex of N, and then to a vertex of M, and then to N and so on. Hence when the cycle returns to u it must be of even length. That is, every cycle of G will have even length.

(iii) implies (i). Lastly, suppose every cycle of G has even length. We pick a vertex in each connected component and paint it the first color, say red. We then successively paint all the vertices as follows: If a vertex is painted red, then any vertex adjacent to it will be painted the second color, say blue. If a vertex is painted blue, then any vertex adjacent to it will be painted red. Since every cycle has even length, no adjacent vertices will be painted the same color. Hence G is 2-colorable, and the theorem is proved.

8.23. Let G be a finite connected planar graph with at least three vertices. Show that G has at least one vertex of degree 5 or less.

Let p be the number of vertices and q the number of edges of G, and suppose $\deg(u) \geq 6$ for each vertex u of G. But $2q$ equals the sum of the degrees of the vertices of G (Theorem 8.1); so $2q \geq 6p$. Therefore

$$q \geq 3p > 3p - 6$$

This contradicts Theorem 8.9. Thus some vertex of G has degree 5 or less.

8.24. Prove Theorem 8.12: A planar graph G is 5-colorable.

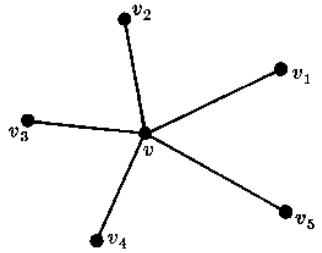


Fig. 8-50

The proof is by induction on the number p of vertices of G. If $p \leq 5$, then the theorem obviously holds. Suppose $p > 5$, and the theorem holds for graphs with less than p vertices. By the preceding problem, G has a vertex v such that $\deg(v) \leq 5$. By induction, the subgraph $G - v$ is 5-colorable. Assume one such coloring. If the vertices adjacent to v use less than the five colors, than we simply paint v with one of the remaining colors and obtain a 5-coloring of G. We are still left with the case that v is adjacent to five vertices which are painted different colors. Say the vertices, moving counterclockwise about v, are $v_1, \ldots, v_5$ and are painted respectively by the colors $c_1, \ldots, c_5$. (See Fig. 8-50.)

Consider now the subgraph H of G generated by the vertices painted c_1 and c_3. Note H includes v_1 and v_3. If v_1 and v_3 belong to different components of H, then we can interchange the colors c_1 and c_3 in the component containing v_1 without destroying the coloring of $G - v$. Then v_1 and v_3 are painted by c_3, c_1 can be chosen to paint v, and we have a 5-coloring of G. On the other hand, suppose v_1 and v_3 are in the same component of H. Then there is a path P from v_1 to v_3 whose vertices are painted either c_1 or c_3. The path P together with the edges $\{v, v_1\}$ and $\{v, v_3\}$ form a cycle C which encloses either v_2 or v_4. Consider now the subgraph K generated by the vertices painted c_3 or c_4. Since C encloses v_2 or v_4, but not both, the vertices v_2 and v_4 belong to different components of K. Thus we can interchange the colors c_2 and c_4 in the component containing v_2 without destroying the coloring of $G - v$. Then v_2 and v_4 are painted by c_4, and we can choose c_2 to paint v and obtain a 5-coloring of G. Thus G is 5-colorable and the theorem is proved.

SEQUENTIAL REPRESENTATION OF GRAPHS

8.25. Find the adjacency matrix $A = [a_{ij}]$ of each graph G in Fig. 8-51.

Set $a_{ij} = n$ if there are n edges $\{v_i, v_j\}$ and $a_{ij} = 0$ otherwise. Hence:

$$(a)\quad A=\begin{bmatrix}0&1&0&1\\1&0&1&1\\0&1&0&1\\1&1&1&0\end{bmatrix};\qquad (b)\quad A=\begin{bmatrix}1&0&0&1\\0&0&2&1\\0&2&0&0\\1&1&0&1\end{bmatrix}$$

[Since (a) has no multiple edges and no loops, the entries in A are either 0 or 1, and are 0 on the diagonal.]

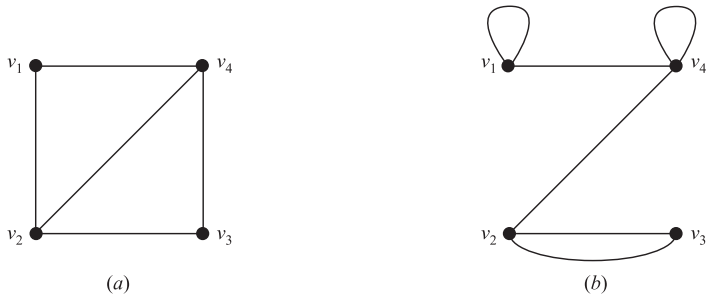


Fig. 8-51

8.26. Draw the graph G corresponding to each adjacency matrix:

$$(a)\quad A=\begin{bmatrix}0&1&0&1&0\\1&0&0&1&1\\0&0&0&1&1\\1&1&1&0&1\\0&1&1&1&0\end{bmatrix};\qquad (b)\quad A=\begin{bmatrix}1&3&0&0\\3&0&1&1\\0&1&2&2\\0&1&2&0\end{bmatrix}$$

(a) Since A is a 5-square matrix, G has five vertices, say, $v_1, v_2 \ldots, v_5$. Draw an edge from v_i to v_j when $a_{ij} = 1$. The graph appears in Fig. 8-52(a).

(b) Since A is a 4-square matrix, G has four vertices, say, $v_1, \ldots, v_4$. Draw n edges from v_i to v_j when $a_{ij} = n$. Also, draw n loops at v_i when $a_{ii} = n$. The graph appears in Fig. 8-52(b).

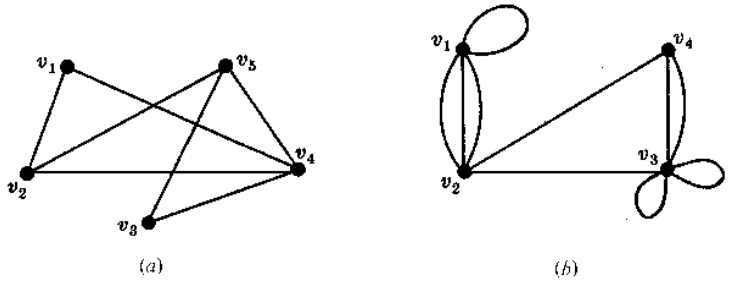


Fig. 8-52

8.27. Consider the weighted graph G in Fig. 8-53. Suppose the vertices are stored in an array DATA as follows:

$$\text{DATA: } A, B, C, X, Y$$

Find the weight matrix $W = (w_{ij})$ of the graph G.

The vertices are numbered according to the way they are stored in array DATA; that is, $v_1 = A$, $v_2 = B, \ldots, v_5 = Y$. Then set $w_{ij} = w$ where w is the weight of the edge from v_i to v_j. Thus,

$$W = \begin{bmatrix} 0 & 6 & 0 & 4 & 1 \\ 6 & 0 & 5 & 0 & 8 \\ 0 & 5 & 0 & 0 & 2 \\ 4 & 0 & 0 & 0 & 3 \\ 1 & 8 & 2 & 3 & 0 \end{bmatrix}$$

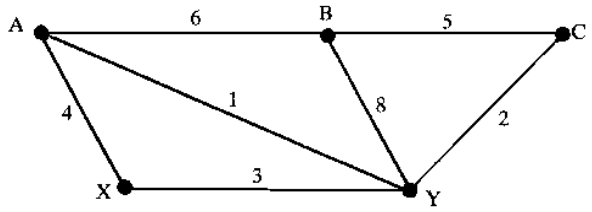


Fig. 8-53

LINKED REPRESENTATION OF GRAPHS

8.28. A graph G with vertices $A, B, \ldots, F$ is stored in memory using a linked representation with a vertex file and an edge file as in Fig. 8-54.

(*a*) List the vertices in the order they appear in memory.

(*b*) Find the adjacency list adj (v) of each vertex v of G.

Vertex file

		1	2	3	4	5	6	7	8
	VERTEX	*B*		*F*	*D*	*A*		*C*	*E*
START 4	NEXT-V	3		5	1	8		0	7
	PTR	9		4	7	6		5	12

Edge file

	1	2	3	4	5	6	7	8	9	10	11	12	13	14
ADJ	4	4	1	8	8	1	5	3	5	8	4	7		
NEXT	8	0	10	0	0	2	3	0	11	0	0	1		

Fig. 8-54

(*a*) Since START = 4, the list begins with the vertex D. The NEXT-V tells us to go to $1(B)$, then $3(F)$, then $5(A)$, then $8(E)$, and then $7(C)$; that is,

$$D, \quad B, \quad F, \quad A, \quad E, \quad C$$

(*b*) Here adj $(D) = [5(A), 1(B), 8(E)]$. Specifically, PTR$[4(D)] = 7$ and ADJ$[7] = 5(A)$ tells us that adj (D) begins with A. Then NEXT$[7] = 3$ and ADJ$[3] = 1(B)$ tells us that B is the next vertex in adj (D). Then NEXT$[3] = 10$ and ADJ$[10] = 8(E)$ tells us that E in the next vertex in adj (D). However, NEXT$[10] = 0$ tells us that there are no more neighbors of D. Similarly.

$$\text{adj}\,(B) = [A, D], \quad \text{adj}\,(F) = [E], \quad \text{adj}\,(A) = [B, D], \quad \text{adj}\,(E) = [C, D, F], \quad \text{adj}\,(C) = [E]$$

In other words, the following is the adjacency structure of G:

$$G = [A{:}B, D; \quad B{:}A, D; \quad C{:}E; \quad D{:}A, B, E; \quad E{:}C, D, F; \quad F{:}E]$$

8.29. Draw the diagram of the graph G whose linked representation appears in Fig. 8-54.

Use the vertex list obtained in Problem 8.28(a) and the adjacency lists obtained in Problem 8.28(b) to draw the graph of G as in Fig. 8-55.

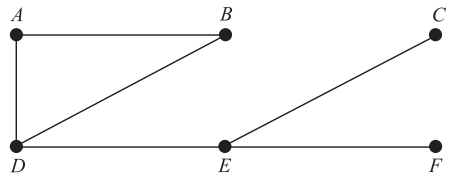


Fig. 8-55

8.30. Exhibit the adjacency structure (AS) of the graph G in: (a) Fig. 8-31; (b) Fig. 8-32.

The adjacency structure of a graph G consists of the adjacency lists of the vertices where we use a colon":" to separate a vertex from its adjacency list, and a semicolon ";" to separate the different lists. Thus:

(a) $G = [A{:}B, C, D;\quad B{:}A, C, E;\quad C{:}A, B, D, E;\quad D{:}A, C;\quad E{:}B, C]$

(b) $G = [A{:}B, D;\quad B{:}A, C, E;\quad C{:}B, E, F;\quad D{:}A, E;\quad E{:}B, C, D, F;\quad F{:}C, E]$

GRAPH ALGORITHMS

8.31. Consider the graph G in Fig. 8-56.

(a) Find the adjacency structure of G.

(b) Find the order the vertices of G are processed using a DFS (depth-first search) algorithm beginning at vertex A.

(a) List the neighbors of each vertex as follows:

$$G = [A{:}B, C, D;\quad B{:}A, E;\quad C{:}A;\quad D{:}A, F;\quad E{:}B, F, H;\quad F{:}D, E, G;\quad G{:}F, H;\quad H{:}E, G]$$

(b) During the DFS algorithm, the first vertex N in STACK is processed and the neighbors of N (which have not been previously processed) are then pushed onto STACK. Initially, the beginning vertex A is pushed onto STACK. The following shows the sequence of waiting lists in STACK and the vertices being processed:

Vertex		A	B	E	F	D	G	H	C
STACK	A	BCD	ECD	$FHCD$	$DGHCD$	GHC	HHC	C	

In other words the vertices are processed in the order A, B, E, F, D, G, H, C.

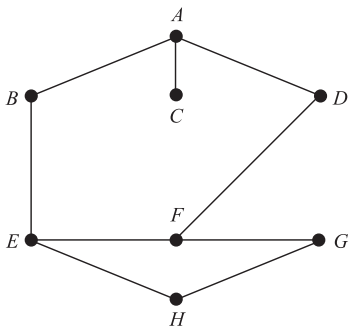


Fig. 8-56

8.32. Find the order the vertices of the graph G in Fig. 8-56 are processed using a BFS (breadth-first search) algorithm beginning at vertex A.

During the BFS algorithm, the first vertex N in QUEUE is processed and the neighbors of N (which have not appeared previously) are then added onto QUEUE. Initially, the beginning vertex A is assigned to QUEUE. The following shows the sequence of waiting lists in QUEUE and the vertices being processed:

Vertex		A	B	C	D	E	F	H	G
QUEUE	A	BCD	CDE	DE	EF	FH	HG	G	

In other words the vertices are processed in the order A, B, C, D, E, F, H, G.

Supplementary Problems

GRAPH TERMINOLOGY

8.33. Consider the graph in Fig. 8-57. Find: (*a*) the degree of each vertex (and verify Theorem 8.1); (*b*) all simple paths from A to G; (*c*) all trails (distinct edges) from B to C; (*d*) $d(A, C)$, the distance from A to C; (*e*) $\text{diam}(G)$, the diameter of G.

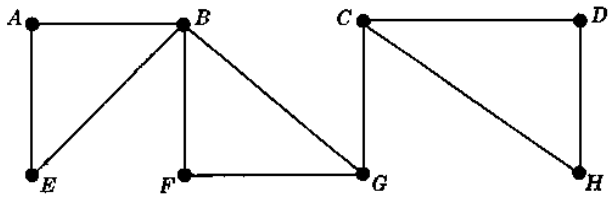


Fig. 8-57

8.34. Consider the graph in Fig. 8-57. Find: (*a*) all cycles, if any; (*b*) all cut points, if any; (*c*) all bridges, if any.

8.35. Consider the graph in Fig. 8-57. Find the subgraph $H(V', E')$ generated by: (*a*) $V' = \{B, C, D, E, F\}$; (*b*) $V' = \{A, C, E, G, H\}$; (*c*) $V' = \{B, D, E, H\}$; (*d*) $V' = \{C, F, G, H\}$.
Which of them are isomorphic? homeomorphic?

8.36. Consider the multigraphs G in Fig. 8-58. (a) Which of them are connected? If they are not, find the number of connected components. (b) Which are cycle-free (without cycles)? If they are not, find the number of cycles. (c) Which are loop-free (without loops)? (d) Which are (simple) graphs?

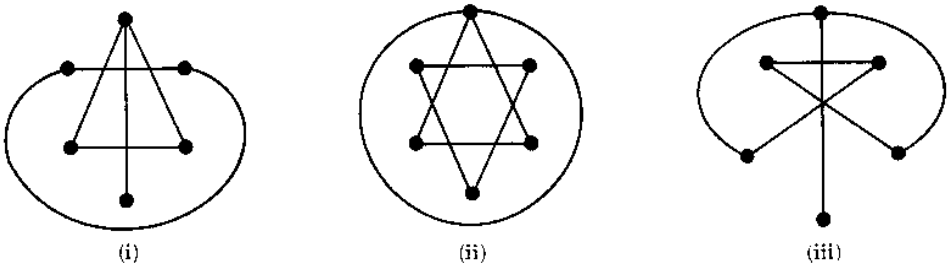


Fig. 8-58

8.37. Suppose a graph G contains two distinct paths from a vertex u to a vertex v. Show that G has a cycle.

8.38. Suppose G is a finite cycle-free graph with at least one edge. Show that G has at least two vertices of degree 1.

8.39. Show that a connected graph G with n vertices must have at least $n - 1$ edges.

8.40. Find the number of connected graphs with four vertices. (Draw them.)

8.41. Let G be a connected graph. Prove:

(a) If G contains a cycle C which contains an edge e; then $G - e$ is still connected.

(b) If $e = \{u, v\}$ is an edge such that $G - e$ is disconnected, then u and v belong to different components of $G - e$.

8.42. Consider the following two steps on a graph G: (1) Delete an edge. (2) Delete a vertex and all edges containing that vertex. Show that every subgraph H of a finite graph G can be obtained by a sequence consisting of these two steps.

TRAVERSABLE GRAPHS, EULER AND HAMILTONIAN CIRCUITS

8.43. Consider each graph G in Fig. 8-59. Find an Euler (traversable) path or an Euler circuit, if it exists. If it does not, why not?

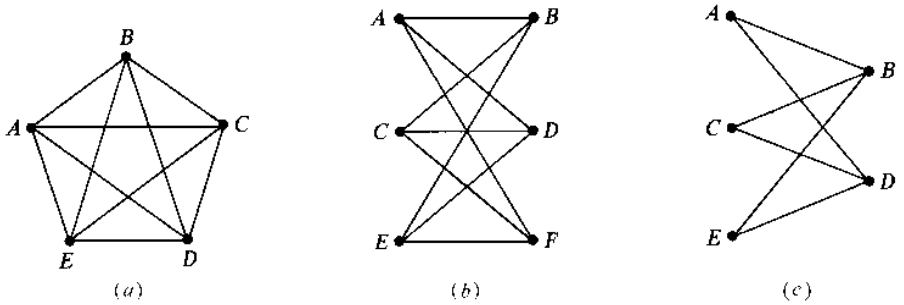


Fig. 8-59

8.44. Consider each graph G in Fig. 8-59. Find a Hamiltonian path or a Hamiltonian circuit, if it exists. If it does not, why not?

8.45. Find the number of Hamiltonian circuits for the graph in Fig. 8-59(a).

8.46. Suppose G and G^* are homeomorphic graphs. Show that G is traversable (Eulerian) if and only if G^* is traversable (Eulerian).

SPECIAL GRAPHS

8.47. Draw two 3-regular graphs with eight vertices.

8.48. Draw two 3-regular graphs with nine vertices.

8.49. Consider the complete graph K_n.

(a) Find the number m of edges in K_n.
(b) Find the degree of each vertex in K_n.
(c) Find those values of n for which K_n is traversable.
(d) Find those vaues of n for which K_n is regular.

8.50. Consider the complete bipartite graph $K_{m,n}$.

(a) Find the diameter of $K_{m,n}$.
(b) Find those $K_{m,n}$ which are traversable.
(c) Which of the graphs $K_{m,n}$ are isomorphic? homeomorphic?

TREES

8.51. Draw all trees with five or fewer vertices.

8.52. Find the number of trees with seven vertices.

8.53. Find the number of spanning trees in Fig. 8-60.

8.54. Find the weight of a minimum spanning tree in Fig. 8-61.

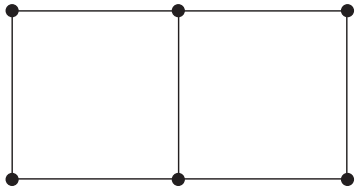


Fig. 8-60

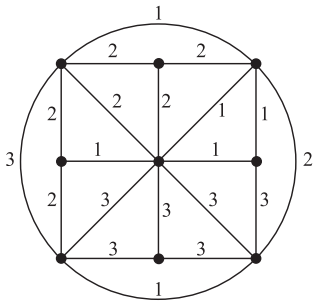


Fig. 8-61

8.55. Show that any tree is a bipartite graph.

8.56. Which complete bipartite graphs $K_{m,n}$ are trees?

PLANAR GRAPHS, MAPS, COLORING

8.57. Draw a planar representation of each graph G in Fig. 8-62, if possible; otherwise show that it has a subgraph homeomorphic to K_5 or $K_{3,3}$.

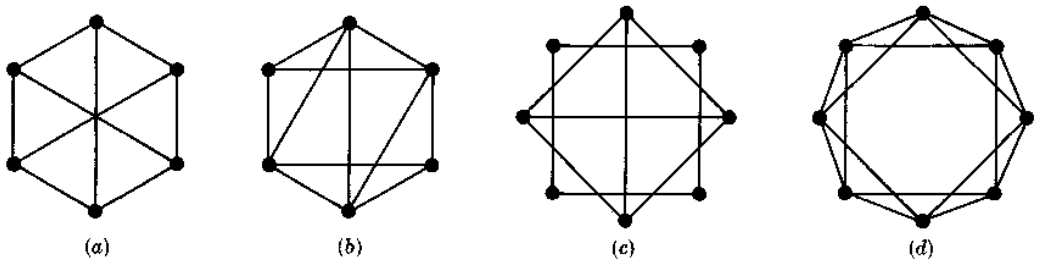


Fig. 8-62

8.58. For the map in Fig. 8-63, find the degree of each region and verify that the sum of the degrees of the regions is equal to twice the number of edges.

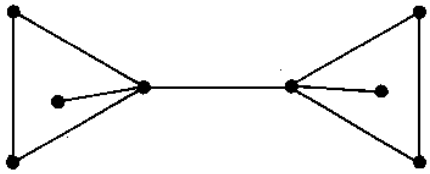


Fig. 8-63

8.59. Count the number V of vertices, the number E of edges, and the number R of regions of each map in Fig. 8-64, and verify Euler's formula.

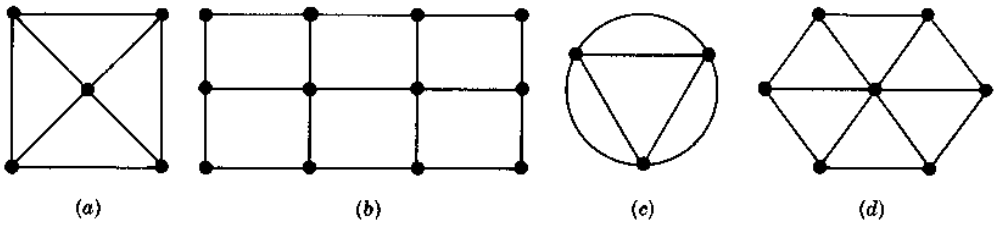


Fig. 8-64

8.60. Find the minimum number of colors needed to paint the regions of each map in Fig. 8-64.

8.61. Draw the map which is dual to each map in Fig. 8-64.

8.62. Use the Welch-Powell algorithm to paint each graph in Fig. 8-65. Find the chromatic number n of the graph.

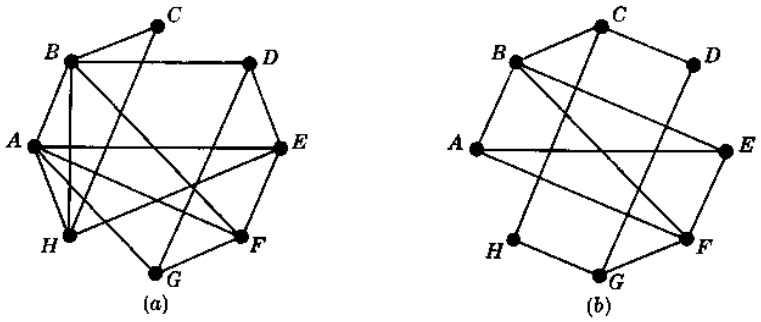


Fig. 8-65

SEQUENTIAL REPRESENTATION OF GRAPHS

8.63. Find the adjacency matrix A of each graph in Fig. 8-66.

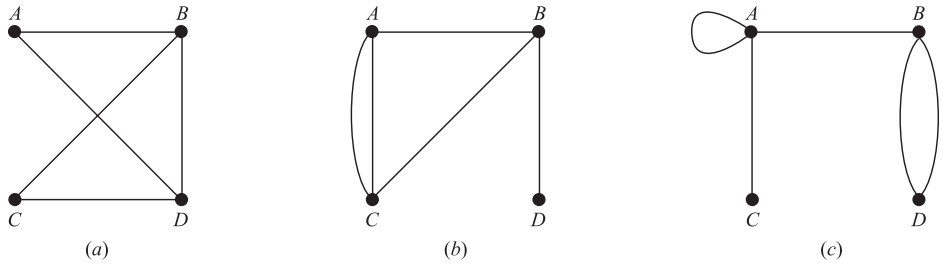


Fig. 8-66

8.64. Draw the multigraph G corresponding to each of the following adjacency matrices:

$$(a)\quad A = \begin{bmatrix} 0 & 2 & 0 & 1 \\ 2 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}; \qquad (b)\quad A = \begin{bmatrix} 1 & 1 & 1 & 2 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 2 \\ 2 & 0 & 2 & 2 \end{bmatrix}$$

8.65. Suppose a graph G is bipartite. Show that one can order the vertices of G so that its adjacency matrix A has the form:

$$A = \begin{bmatrix} 0 & B \\ C & 0 \end{bmatrix}$$

LINKED REPRESENTATION OF GRAPHS

8.66. Suppose a graph G is stored in memory as in Fig. 8-67.

(*a*) List the vertices in the order in which they appear in memory.

(*b*) Find the adjacency structure of G, that is, find the adjacency list adj(v) of each vertex v of G.

Vertex file

		1	2	3	4	5	6	7	8
	VERTEX	*C*		*F*	*E*	*A*		*B*	*D*
START 7	NEXT-V	0		5	1	8		3	4
	PTR	2		11	6	12		4	1

Edge file

	1	2	3	4	5	6	7	8	9	10	11	12
ADJ	7	7	4	5		7	1		8	3	1	7
NEXT	0	10	0	7		0	9		3	0	0	0

Fig. 8-67

8.67. Exhibit the adjacency structure (AS) of each graph G in Fig. 8-59.

8.68. Figure 8-68 shows a graph G representing six cities, $A, B, \ldots, F$, connected by seven numbered highways, $22, 33, \ldots, 88$. Show how G can be maintained in memory using a linked representation with sorted arrays for the cities and the numbered highways. (Note that VERTEX is a sorted array and so the field NEXT-V is not needed.)

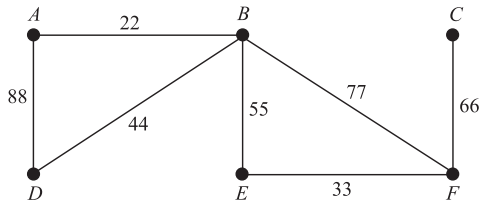


Fig. 8-68

GRAPH ALGORITHMS

8.69. Consider the graph G in Fig. 8-57.

(*a*) Find the adjacency structure of G.

(*b*) Find the order the vertices of G are processed using a DFS (depth-first search) algorithm beginning at: (i) vertex C; (ii) vertex B.

8.70. Find the order the vertices of the graph G in Fig. 8-57 are processed using a BFS (breadth-first search) algorithm beginning at: (*a*) vertex C; (*b*) vertex B.

Answers to Supplementary Problems

8.33. (*a*) $2, 4, 3, 2, 2, 2, 3, 2$; (*b*) ABG, $ABFG$, $AEBG$, $AEBFG$; (*c*) BGC, $BFGC$, $BAEBGC$, $BAEBFGC$; (*d*) 3; (*e*) 4.

8.34. (*a*) $ABEA$, $BFGB$, $CDHC$; (*b*) B, C, G; (*c*) only $\{C, G\}$.

8.35. (*a*) $E' = \{BE, BF, CD\}$; (*b*) $E' = \{AE, FG, GC\}$; (*c*) $E' = \{BE, DH\}$; (*d*) $E' = \{FG, GC, CH\}$.

Also, (*a*) and (*b*) are isomorphic, and (*a*), (*b*), and (*c*) are homeomorphic.

8.36. (*a*) (iii) is connected, (i) and (ii) have two connected components; (*b*) none, (i) 1, (ii) 2, (iii) 1; (*c*) (i) and (iii); (*d*) (iii).

8.38. *Hint*: Consider a maximal simple path α, and show that its endpoints have degree 1.

8.40. There are five of them, as shown in Fig. 8-69.

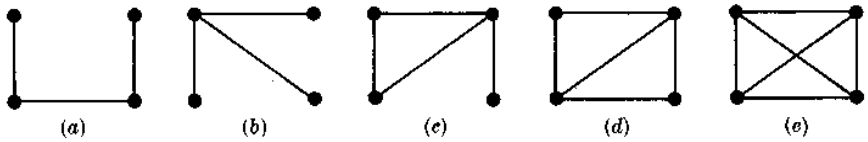


Fig. 8-69

8.42. First delete all edges in G not in H, then delete all vertrices in G not in H.

8.43. (*a*) Eulerian since all vertices are even: *ABCDEACEBDA*. (*b*) None, since four vertices are odd. (*c*) Euler path beginning at B and ending at D (or vice versa): *BADCBED*.

8.44. (*a*) *ABCDEA*; (*b*) *ABCDEFA*; (*c*) none, since B or D must be visited twice in any closed path including all vertices.

8.45. $(5-1)!/2 = 12$.

8.46. *Hint*: Adding a vertex by dividing an edge does not change the degree of the original vertices and simply adds a vertex of even degree.

8.47. The two 3-regular graphs in Fig. 8-70 are not isomorphic since (*b*) has a 5-cycle but (*a*) does not.

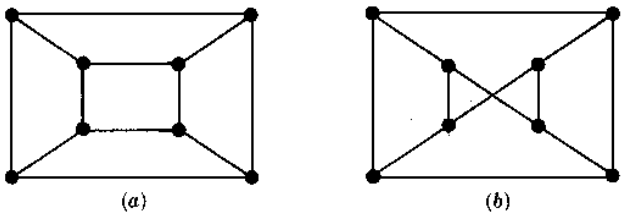


Fig. 8-70

8.48. None. The sum of the degrees of an r-regular graph with s vertices equals rs and it must be even.

8.49. (*a*) $m = C(n,2) = n(n-1)/2$; (*b*) $n-1$; (*c*) $n = 2$ and n odd; (*d*) all n.

8.50. (*a*) $\text{diam}(K_{1,1}) = 1$; all others have diameter 2.

(*b*) $K_{1,1}$, $K_{1,2}$, and all $K_{m,n}$ where m and n are even.

(*c*) None are isomorphic; only $K_{1,1}$ and $K_{1,2}$ are homeomorphic.

8.51. There are eight such trees, as shown in Fig. 8-71. The graph with one vertex and no edges is called the *trivial tree*.

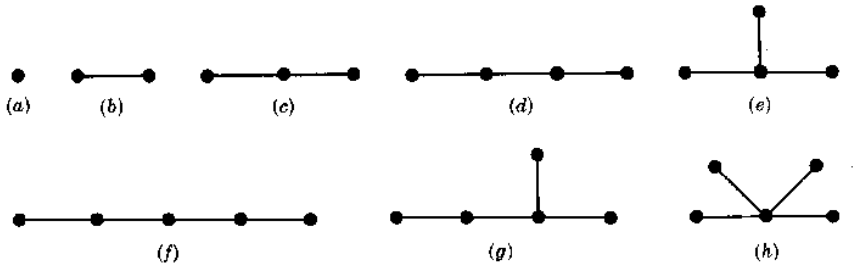


Fig. 8-71

8.52. Ten.

8.53. Fifteen.

8.54. $1 + 1 + 1 + 1 + 1 + 2 + 2 + 3 = 12$.

8.56. $m = 1$.

8.57. Only (*a*) is nonplanar, and $K_{3,3}$ is a subgraph.

8.58. The outside region has degree 8, and the other two regions have degree 5.

8.59. (*a*) 5, 8, 5; (*b*) 12, 17, 7; (*c*) 3, 6, 5; (*d*) 7, 12, 7.

8.60. (*a*) 3; (*b*) 3; (*c*) 2; (*d*) 3.

8.61. See Fig. 8-72.

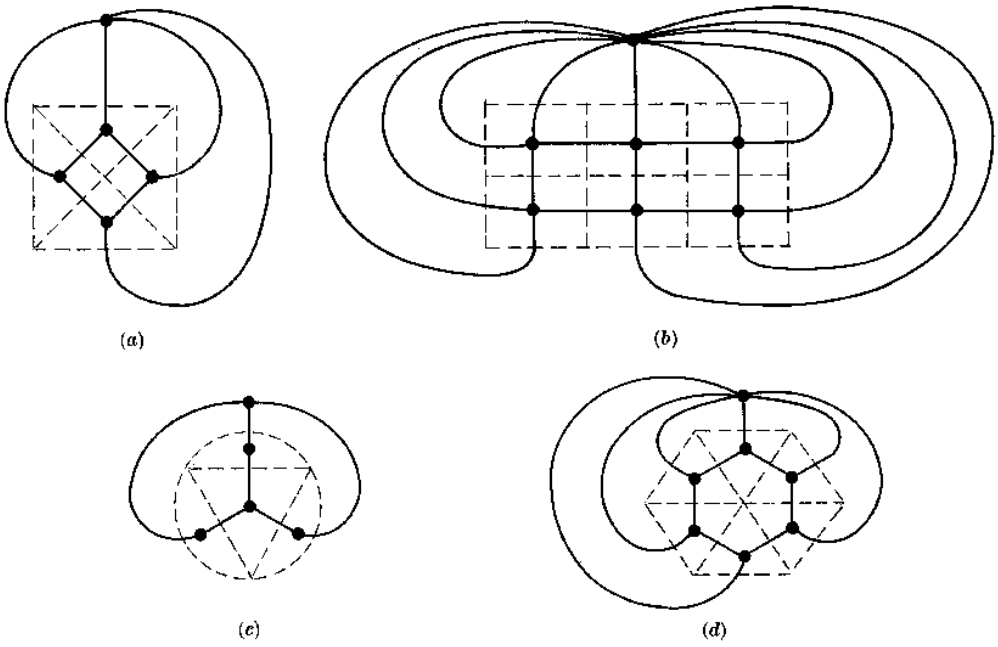


Fig. 8-72

8.62. (*a*) $n = 3$; (*b*) $n = 4$.

8.63. (*a*) $\begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$; (*b*) $\begin{bmatrix} 0 & 1 & 2 & 0 \\ 1 & 0 & 1 & 1 \\ 2 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$; (*c*) $\begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 2 \\ 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \end{bmatrix}$.

8.64. See Fig. 8-73.

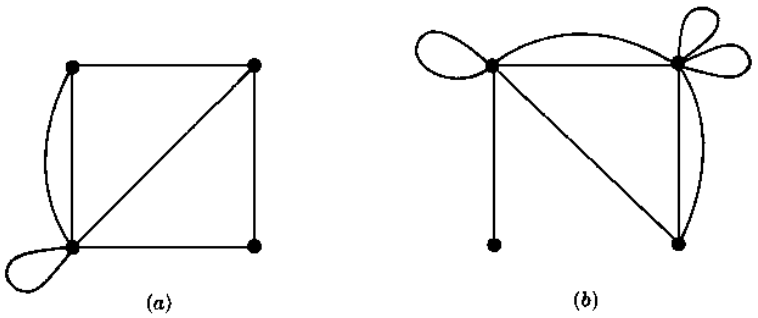


Fig. 8-73

8.65. Let M and N be the two disjoint sets of vertices determining the bipartite graph G. Order the vertices in M first and then those in N.

8.66. (*a*) B, F, A, D, E, C.
(*b*) $G = [A{:}B;\quad B{:}A, C, D, E;\quad C{:}F;\quad D{:}B;\quad E{:}B;\quad F{:}C]$.

8.67. (*a*) Each vertex is adjacent to the other four vertices.
(*b*) $G = [A{:}B, D, F;\quad B{:}A, C, E;\quad C{:}B, D, F;\quad D{:}A, C, E;\quad E{:}B, D, F;\quad F{:}A, C, E]$.
(*c*) $G = [A{:}B, D;\quad B{:}A, C, E;\quad C{:}B, D;\quad D{:}A, C, E;\quad E{:}B, D]$.

8.68. See Fig. 8-74.

Vertex file

	1	2	3	4	5	6	7	8
VERTEX	*A*	*B*	*C*	*D*	*E*	*F*		
PTR	1	2	9	14	8	12		

Edge file

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
NUMBER	22	22	33	33	44	44	55	55	66	66	77	77	88	88	
ADJ	2	1	6	5	4	2	5	2	6	3	6	2	4	1	
NEXT	13	5	0	0	7	0	11	3	0	4	0	10	0	6	

Fig. 8-74

8.69. (*a*) $G = [A{:}B, E;\quad B{:}A, E, F, G;\quad C{:}D, G, H;\quad D{:}C, H;\quad E{:}A, B;\quad F{:}B, G;\quad G{:}B, C, F;\quad H{:}C, D]$.
(*b*) (i) C, D, H, G, B, A, E, F; (ii) B, A, E, F, G, C, D, H.

8.70. (*a*) C, D, G, H, B, F, A, E; (*b*) B, A, E, F, G, C, D, H.

© The McGraw–Hill Companies, 2004

Chapter 9

Directed Graphs

9.1 INTRODUCTION

Directed graphs are graphs in which the edges are one-way. Such graphs are frequently more useful in various dynamical systems such as digital computers or flow systems. However, this added feature makes it more difficult to determine certain properties of the graph. That is, processing such graphs may be similar to traveling in a city with many one-way streets.

Directed graphs have already appeared in Chapter 3 on relations. One may view certain directed graphs as (binary) relations. For this reason, some texts discuss directed graphs in the context of relations. In fact, here we will present an efficient algorithm for finding the transitive closure of a relation.

This chapter gives the basic definitions and properties of directed graphs. Many of the definitions will be similar to those in the preceding chapter on (nondirected) graphs. However, for pedagogical reasons, this chapter will be mainly independent from the preceding chapter.

9.2 DIRECTED GRAPHS

A *directed graph* G or *digraph* (or simply *graph*) consists of two things:

(i) A set V whose elements are called *vertices*, *nodes*, or *points*.

(ii) A set E of *ordered* pairs (u, v) of vertices called *arcs* or *directed edges* or simply *edges*.

We will write $G(V, E)$ when we want to emphasize the two parts of G. We will also write $V(G)$ and $E(G)$ to denote, respectively, the set of vertices and the set of edges of a graph G. (If it is not explicitly stated, the context usually determines whether or not a graph G is a directed graph.)

Suppose $e = (u, v)$ is a directed edge in a digraph G. Then the following terminology is used:

(a) e *begins* at u and *ends* at v.
(b) u is the *origin* or *initial point* of e, and v is the *destination* or *terminal point* of e.
(c) v is a *successor* of u.
(d) u is *adjacent to* v, and v is *adjacent from* u.

If $u = v$, then e is called a *loop*.

The set of all successors of a vertex u is important; it is denoted and formally defined by

$$\text{succ}\ (u) = \{v \in V\text{: there exists } (u, v) \in E\}$$

It is called the *successor list* or *adjacency list* of u.

A *picture* of a directed graph G is a representation of G in the plane. That is, each vertex u of G is represented by a dot (or small circle), and each (directed) edge $e = (u, v)$ is represented by an arrow or directed curve from the initial point u of e to the terminal point v. One usually presents a digraph G by its picture rather than explicitly listing its vertices and edges.

If the edges and/or vertices of a directed graph G are labeled with some type of data, then G is called a *labeled directed graph*.

A directed graph $G(V, E)$ is said to be *finite* if its set V of vertices and its set E of edges are finite.

EXAMPLE 9.1

(a) Consider the directed graph G pictured in Fig. 9-1. It consists of four vertices and seven edges as follows:

$$V(G) = \{A, B, C, D\}$$
$$E(G) = \{e_1, \ldots, e_7\} = \{(A, D), (B, A), (B, A), (D, B), (B, C), (D, C), (B, B)\}$$

The edges e_2 and e_3 are said to be *parallel* since they both begin at B and end at A. The edge e_7 is a *loop* since it begins and ends at B.

(*b*) Suppose three boys, A, B, C, are throwing a ball to each other such that A always throws the ball to B, but B and C are just as likely to throw the ball to A as they are to each other. Figure 9-2 illustrates this dynamical system, where edges are labeled with the respective probabilities, i.e., A throws the ball to B with probability 1, B throws the ball to A and C each with probability $\frac{1}{2}$, and C throws the ball to A and B each with probability $\frac{1}{2}$.

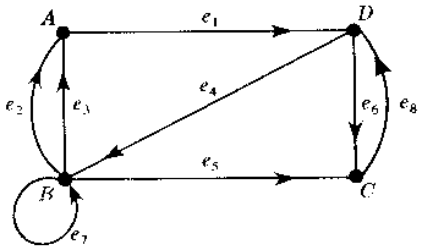


Fig. 9-1

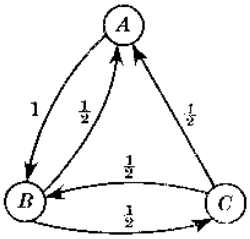


Fig 9-2

Subgraphs

Let $G = G(V, E)$ be a directed graph, and let V' be a subset of set V of vertices of G. Suppose E' is a subset of E such that the endpoints of the edges in E' belong to V'. Then $H(V', E')$ is a directed graph, and it is called a *subgraph* of G. In particular, if E' contains all the edges in E whose endpoints belong to V', then $H(V', E')$ is called the subgraph of G *generated* or *determined* by V'. For example, consider the graph $G = G(V, E)$ in Fig. 9-1. Let

$$V' = \{B, C, D\} \qquad \text{and} \qquad E' = \{e_4, e_5, e_6, e_7\} = \{(D, B), (B, C), (D, C), (B, B)\}$$

Then $H(V', E')$ is the subgraph of G determine by the vertex set V'.

9.3 BASIC DEFINITIONS

This section discusses the questions of degrees of vertices, paths, and connectivity in a directed graph.

Degrees

Suppose G is a directed graph. The *outdegree* of a vertex v of G, written outdeg(v), is the number of edges beginning at v, and the *indegree* of v, written indeg(v), is the number of edges ending at v. Since each edge begins and ends at a vertex we immediately obtain the following theorem.

Theorem 9.1: The sum of the outdegrees of the vertices of a digraph G equals the sum of the indegrees of the vertices, which equals the number of edges in G.

A vertex v with zero indegree is called a *source*, and a vertex v with zero outdegree is called a *sink*.

EXAMPLE 9.2 Consider the graph G in Fig. 9-1. We have:

$$\begin{aligned} &\text{outdeg}(A) = 1, \quad &&\text{outdeg}(B) = 4, \quad &&\text{outdeg}(C) = 0, \quad &&\text{outdeg}(D) = 2 \\ &\text{indeg}(A) = 2, \quad &&\text{indeg}(B) = 2, \quad &&\text{indeg}(C) = 2, \quad &&\text{indeg}(D) = 1 \end{aligned}$$

As expected, the sum of the outdegrees equals the sum of the indegrees, which equals the number 7 of edges. The vertex C is a sink since no edge begins at C. The graph has no sources.

Paths

Let G be a directed graph. The concepts of path, simple path, trail and cycle carry over from nondirected graphs to G except that the directions of the edges must agree with the direction of the path. Specifically:

(i) *A* (*directed*) *path* P in G is an alternating sequence of vertices and directed edges, say,

$$P = (v_0, e_1, v_1, e_2, v_2, \ldots, e_n, v_n)$$

such that each edge e_i begins at v_{i-1} and ends at v_i. If there is no ambiguity, we denote P by its sequence of vertices or its sequence of edges.

(ii) The *length* of the path P is n, its number of edges.

(iii) A *simple path* is a path with distinct vertices. A *trail* is a path with distinct edges.

(iv) A *closed path* has the same first and last vertices.

(v) A *spanning path* contains all the vertices of G.

(vi) A *cycle* (or *circuit*) is a closed path with distinct vertices (except the first and last).

(vii) A *semipath* is the same as a path except the edge e_i may begin at v_{i-1} or v_i and end at the other vertex. *Semitrails* and *semisimple paths* are analogously defined.

A vertex v is *reachable* from a vertex u if there is a path from u to v. If v is reachable from u, then (by eliminating redundant edges) there must be a simple path from u to v.

EXAMPLE 9.3 Consider the graph G in Fig. 9-1.

(*a*) The sequence $P_1 = (D, C, B, A)$ is a semipath but not a path since (C, B) is not an edge; that is, the direction of $e_5 = (C, B)$ does not agree with the direction of P_1.

(*b*) The sequence $P_2 = (D, B, A)$ is a path from D to A since (D, B) and (B, A) are edges. Thus A is reachable from D.

Connectivity

There are three types of connectivity in a directed graph G:

(i) G is *strongly connected* or *strong* if, for any pair of vertices u and v in G, there is a path from u to v and a path from v to u, that is, each is reachable from the other.

(ii) G is *unilaterally connected* or *unilateral* if, for any pair of vertices u and v in G, there is a path from u to v or a path from v to u, that is, one of them is reachable from the other.

(iii) G is *weakly connected* or *weak* if there is a semipath between any pair of vertices u and v in G.

Let G' be the (nondirected) graph obtained from a directed graph G by allowing all edges in G to be nondirected. Clearly, G is weakly connected if and only if the graph G' is connected.

Observe that strongly connected implies unilaterally connected, and that unilaterally connected implies weakly connected. We say that G is *strictly unilateral* if it is unilateral but not strong, and we say that G is *strictly weak* if it is weak but not unilateral.

Connectivity can be characterized in terms of spanning paths as follows:

Theorem 9.2: Let G be a finite directed graph. Then:

(i) G is strong if and only if G has a closed spanning path.

(ii) G is unilateral if and only if G has a spanning path.

(iii) G is weak if and only if G has a spanning semipath.

EXAMPLE 9.4 Consider the graph G in Fig. 9-1. It is weakly connected since the underlying nondirected graph is connected. There is no path from C to any other vertex (i.e., C is a sink), so G is not strongly connected. However, $P = (B, A, D, C)$ is a spanning path, so G is unilaterally connected.

Graphs with sources and sinks appear in many applications (e.g., flow diagrams and networks). A sufficient condition for such vertices to exist follows.

Theorem 9.3: Suppose a finite directed graph G is cycle-free, that is, contains no (directed) cycles. Then G contains a source and a sink.

Proof: Let $P = (v_0, v_1, \ldots, v_n)$ be a simple path of maximum length, which exists since G is finite. Then the last vertex v_n is a sink; otherwise an edge (v_n, u) will either extend P or from a cycle if $u = v_i$ for some i. Similarly, the first vertex v_0 is a source.

9.4 ROOTED TREES

Recall that a tree graph is a connected cycle-free graph, that is, a connected graph without any cycles. A *rooted tree* T is a tree graph with a designated vertex r called the *root* of the tree. Since there is a unique simple path from the root r to any other vertex v in T, this determines a direction to the edges of T. Thus T may be viewed as a directed graph. We note that any tree may be made into a rooted tree by simply selecting one of the vertices as the root.

Consider a rooted tree T with root r. The length of the path from the root r to any vertex v is called the *level* (or *depth*) of v, and the maximum vertex level is called the *depth* of the tree. Those vertices with degree 1, other than the root r, are called the *leaves* of T, and a directed path from a vertex to a leaf is called a *branch*.

One usually draws a picture of a rooted tree T with the root at the top of the tree. Figure 9-3 show a rooted tree T with root r and 10 other vertices. The tree has five leaves, d, f, h, i, and j. Observe that:

$$\text{level}\,(a) = 1, \qquad \text{level}\,(f) = 2, \qquad \text{level}\,(j) = 3$$

Furthermore, the depth of the tree is 3.

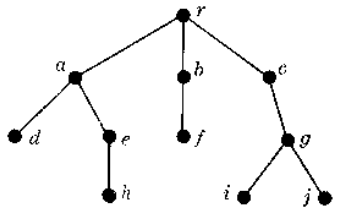


Fig. 9-3

The fact that a rooted tree T gives a direction to the edges means that we can give a precedence relationship between the vertices. Specifically, we will say that a vertex u *precedes* a vertex v or that v *follows* u if there is a (directed) path from v to u. In particular, we say that v *immediately follows* u if (u, v) is an edge, that is, if v follows u and is adjacent to u. We note that every vertex v, other than the root, immediately follows a unique vertex, but that v can be immediately followed by more than one vertex. For example, in Fig. 9-3, the vertex j follows c but immediately follows g. Also, both i and j immediately follow g.

A rooted tree T is also a useful device to enumerate all the logical possibilities of a sequence of events where each event can occur in a finite number of ways. This is illustrated in the following example.

EXAMPLE 9.5 Suppose Marc and Erik are playing a tennis tournament such that the first person to win two games in a row or who wins a total of three games wins the tournament. Find the number of ways the tournament can proceed.

The rooted tree in Fig. 9-4 (where the root is on the left) shows the various ways that the tournament could proceed. There are 10 leaves which correspond to the 10 ways that the tournament can occur:

MM, MEMM, MEMEM, MEMEE, MEE, EMM, EMEMM, EMEME, EMEE, EE

Specifically, the path from the root to the leaf describes who won which games in the particular tournament.

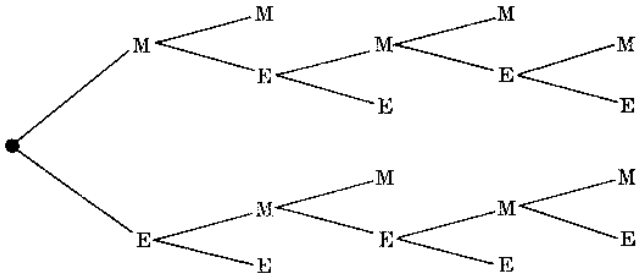


Fig. 9-4

Ordered Rooted Trees

Consider a rooted tree T in which the edges leaving each vertex are ordered. Then we have the concept of an *ordered rooted tree*. One can systematically label (or *address*) the vertices of such a tree as follows: We first assign 0 to the root r. We next assign $1, 2, 3, \ldots$ to the vertices immediately following r according as the edges were ordered. We then label the remaining vertices in the following way. If a is the label of a vertex v, then $a.1$, $a.2, \ldots$ are assigned to the vertices immediately following v according as the edges were ordered. We illustrate this address system in Fig. 9-5, where edges are pictured from left to right according to their order. Observe that the number of decimal points in any label is one less than the level of the vertex. We will refer to this labeling system as the *universal address system* for an ordered rooted tree.

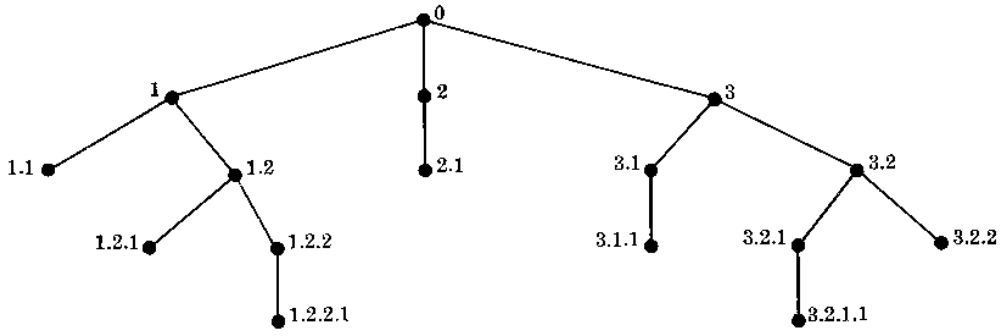
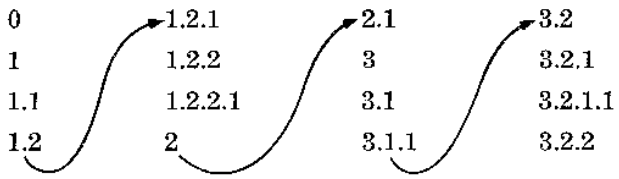


Fig. 9-5

The universal address system gives us an important way of linearly describing (or storing) an ordered rooted tree. Specifically, given addresses a and b, we let $a < b$ if a is an *initial segment* of b, i.e., if $b = a.c$, or if there exist positive integers m and n with $m < n$ such that

$$a = r.m.s \qquad \text{and} \qquad b = r.n.t$$

This order is called *lexicographic order* since it is similar to the way words are arranged in a dictionary. For example, the addresses in Fig. 7-5 are linearly ordered as follows:



This lexicographic order is identical to the order obtained by moving down the leftmost branch of the tree, then the next branch to the right, then the second branch to the right, and so on.

Algebraic Expressions and Polish Notation

Any algebraic expression involving binary operations, for example, addition, subtraction, multiplication and division, can be represented by an ordered rooted tree. For example, Fig. 9-6(*a*) represents the arithmetic expression

$$(a - b)/((c \times d) + e) \tag{9.1}$$

Observe that the variables in the expression, a, b, c, d and e, appear as leaves, and the operations appear as the other vertices. The tree must be ordered since $a - b$ and $b - a$ yield the same tree but not the same ordered tree.

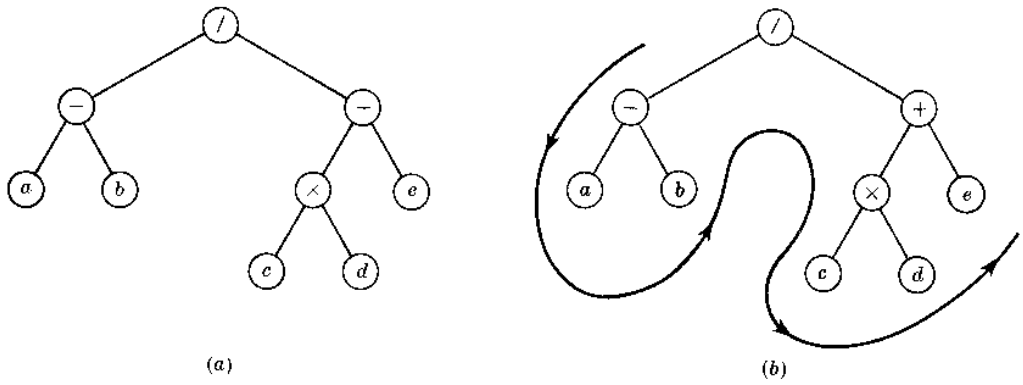


Fig. 9-6

The Polish mathematician Lukasiewicz observed that by placing the binary operational symbol before its arguments, e.g.,

$$+ab \text{ instead of } a + b \qquad \text{and} \qquad /cd \text{ instead of } c/d$$

one does not need to use any parentheses. This notation is called *Polish notation* in *prefix form*. (Analogously, one can place the symbol after its arguments, called *Polish notation* in *postfix form*.) Rewriting (9.1) in prefix form we obtain

$$/ - ab + \times cde$$

Observe that this is precisely the lexicographic order of the vertices in its tree which can be obtained by scanning the tree as in Fig. 9-6(*b*).

9.5 SEQUENTIAL REPRESENTATION OF DIRECTED GRAPHS

There are two main ways of maintaining a directed graph G in the memory of a computer. One way, called the *sequential representation* of G, is by means of its adjacency matrix A. The other way, called the *linked representation* of G, is by means of linked lists of neighbors. This section covers the first representation and shows how the adjacency matrix A of G can be used to easily answer certain questions of connectivity in G. The linked representation will be covered in Section 9.7.

Suppose a graph G has m vertices (nodes) and n edges. We say G is *dense* if $m = O(n^2)$ and *sparse* if $m = O(n)$ or even if $m = O(n \log n)$. The matrix representation of G is usually used when G is dense, and linked lists are usually used when G is sparse. Regardless of the way one maintains a graph G in memory, the graph G is normally input into the computer by its formal definition, that is, as a collection of vertices and a collection of edges (pairs of vertices).

Remark: In order to avoid special cases of our results, we will always assume, unless otherwise stated, that $m > 1$ where m is the number of vertices in our graph G. Therefore, G cannot be connected if G has no edges.

Digraphs and Relations, Adjacency Matrix

Let $G(V, E)$ be a *simple* directed graph, that is, a graph without parallel edges. Then E is simply a subset of $V \times V$, and hence E is a relation on V. Conversely, if R is a relation on a set V, then $G(V, R)$ is a simple directed graph. Thus the concepts of relations on a set and simple directed graphs are one and the same. In fact, in Chapter 2, we already introduced the directed graph corresponding to a relation on a set.

Suppose G is a simple directed graph with m vertices, and suppose the vertices of G have been ordered and are called $v_1, v_2, \ldots, v_m$. Then the *adjacency matrix* $A = [a_{ij}]$ of G is the $m \times m$ matrix defined as follows:

$$a_{ij} = \begin{cases} 1 & \text{if there is an edge } (v_i, v_j) \\ 0 & \text{otherwise} \end{cases}$$

Such a matrix A, which contains entries of only 0 or 1, is called a *bit matrix* or a *Boolean matrix*.

The adjacency matrix A of the graph G does depend on the ordering of the vertices of G; that is, a different ordering of the vertices may result in a different adjacency matrix. However, the matrices resuting from two different orderings are closely related in that one can be obtained from the other by simply interchanging rows and columns. Unless otherwise stated, we assume that the vertices of our matrix have a fixed ordering.

Remark 1: The adjacency matrix $A = [a_{ij}]$ may be extended to directed graphs with parallel edges by setting

$$a_{ij} = \text{the number of edges beginning at } v_i \text{ and ending at } v_j$$

Then the entries of A will be nonnegative integers. Conversely, every $m \times m$ matrix A with nonnegative integer entries uniquely defines a directed graph with m vertices.

Remark 2: If G is an undirected graph, then the adjacency matrix A of G will be a symmetric matrix, i.e., $a_{ij} = a_{ji}$ for every i and j. This follows from the fact that each undirected edge $\{u, v\}$ corresponds to two directed edges (u, v) and (v, u).

EXAMPLE 9.6 Consider the directed graph G in Fig. 9-7 with vertices X, Y, Z, W. Suppose the vertices are ordered as follows:

$$v_1 = X, \qquad v_2 = Y, \qquad v_3 = Z, \qquad v_4 = W$$

Then the adjacency matrix A of G follows:

$$A = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}$$

Note that the number of 1's in A is equal to the number (8) of edges.

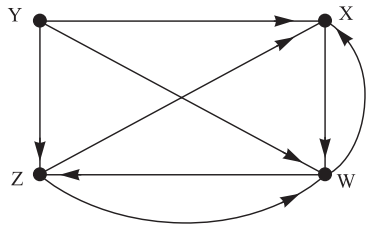


Fig. 9-7

Consider the powers A, A^2, $A^3, \ldots$ of the adjacency matrix $A = [a_{ij}]$ of a graph G. We will use the notation:

$$a_K(i,j) = \text{the } ij \text{ entry in the matrix } A^K$$

Note that $a_1(i,j) = a_{ij}$ gives the number of paths of length 1 from vertex v_i to vertex v_j. One can show that $a_2(i,j)$ gives the number of paths of length 2 from v_i to v_j. In fact, we prove in Problem 9.14 the following general result.

Proposition 9.4: Let A be the adjacency matrix of a graph G. Then $a_K(i,j)$, the ij entry in the matrix A^K, gives the number of paths of length K from v_i to v_j.

EXAMPLE 9.7 Consider again the graph G in Fig. 9-7 whose adjacency matrix A is given in Example 9.6. The powers A^2, A^3, and A^4 of A follow:

$$A^2 = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 2 & 0 & 1 & 2 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 2 \end{bmatrix}, \qquad A^3 = \begin{bmatrix} 1 & 0 & 0 & 2 \\ 3 & 0 & 2 & 3 \\ 2 & 0 & 1 & 2 \\ 2 & 0 & 2 & 1 \end{bmatrix}, \qquad A^4 = \begin{bmatrix} 2 & 0 & 2 & 1 \\ 5 & 0 & 3 & 5 \\ 3 & 0 & 2 & 3 \\ 3 & 0 & 1 & 4 \end{bmatrix}$$

Observe that $a_2(4,1) = 1$, so there is a path of length 2 from v_4 to v_1. Also, $a_3(2,3) = 2$, so there are two paths of length 3 from v_2 to v_3; and $a_4(2,4) = 5$, so there are five paths of length 4 from v_2 to v_4. (Here, $v_1 = X$, $v_2 = Y$, $v_3 = Z$, $v_4 = W$.)

Remark: Suppose A is the adjacency matrix of a graph G, and suppose we now define the matrix B_r as follows:

$$B_r = A + A^2 + A^3 + \cdots + A^r$$

Then the ij entry of the matrix B_r gives the number of paths of length r or less from vertex v_i to vertex v_j.

Path Matrix

Let $G = G(V, E)$ be a simple directed graph with m vertices $v_1, v_2, \ldots, v_m$. The *path matrix* or *reachability matrix* of G is the m-square matrix $P = (p_{ij})$ defined as follows:

$$p_{ij} = \begin{cases} 1 & \text{if there is a path from } v_i \text{ to } v_j \\ 0 & \text{otherwise} \end{cases}$$

(The next subsection shows that the path matrix P may be viewed as the transitive closure of the relation E on V.)

Suppose now that there is a path from vertex v_i to vertex v_j in a graph G with m vertices. Then there must be a simple path from v_i to v_j when $v_i \neq v_j$, or there must be a cycle from v_i to v_j when $v_i = v_j$. Since G has m vertices, such a simple path must have length $m - 1$ or less, or such a cycle must have length m or less. This means that there is a nonzero ij entry in the matrix

$$B_m = A + A^2 + A^3 + \cdots + A^m$$

where A is the adjacency matrix of G. Accordingly, the path matrix P and B_m have the same nonzero entries. We state this result formally.

Proposition 9.5: Let A be the adjacency matrix of a graph G with m vertices, and let

$$B_m = A + A^2 + A^3 + \cdots + A^m$$

Then the path matrix P and B_m have the same nonzero entries.

Recall that a directed graph G is said to be *strongly connected* if, for any pair of vertices u and v in G, there is a path from u to v and from v to u. Accordingly, G is strongly connected if and only if the path matrix P of G has no zero entries. This fact together with Proposition 9.5 gives the following result.

Proposition 9.6: Let A be the adjacency matrix of a graph G with m vertices, and let

$$B_m = A + A^2 + A^3 + \cdots + A^m$$

Then G is strongly connected if and only if B_m has no zero entries.

EXAMPLE 9.8 Consider the graph G with $m = 4$ vertices in Fig. 9-7 where we let $v_1 = X$, $v_2 = Y$, $v_3 = Z$, $v_4 = W$. Adding the matrices A, A^2, A^3, A^4 in Examples 9.6 and 9.7, we obtain the following matrix B_4, and, replacing the nonzero entries in B_4 by 1, we obtain the path (reachability) matrix P of the graph G:

$$B_4 = \begin{bmatrix} 4 & 0 & 3 & 4 \\ 11 & 0 & 7 & 11 \\ 7 & 0 & 4 & 7 \\ 7 & 0 & 4 & 7 \end{bmatrix} \quad \text{and} \quad P = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix}$$

Examining the matrix B_4 or P, we see zero entries; hence G is not strongly connected. In particular, we see that the vertex $v_2 = Y$ is not reachable from any of the other vertices.

Remark: The adjacency matrix A and the path matrix P of a graph G may be viewed as logical (Boolean) matrices where 0 represents "False" and 1 represents "True". Thus the logical operations of $\wedge$ (AND) and $\vee$ (OR), whose values appear in Fig. 9-8, may be applied to the entries of A and P. These operations will be used in the next section.

$\wedge$	0	1
0	0	0
1	0	1

(a) AND.

$\vee$	0	1
0	0	1
1	1	1

(b) OR.

Fig. 9-8

Transitive Closure and the Path Matrix

Let R be a relation on a finite set V with m elements. As noted above, the relation R may be identified with the simple directed graph $G = G(V, R)$. Recall (Section 2.5) that the composition relation $R^2 = R \circ R$ is defined by

$$R^2 = \{(u, v): \exists\ w \in V \text{ such that } (u, w) \in R \text{ and } (w, v) \in R\}$$

In other words, R^2 consists of all pairs (u, v) such that there is a path of length 2 from u to v. Similarly:

$$R^K = \{(u, v): \text{there is a path of length } K \text{ from } u \text{ to } v\}.$$

The transitive closure R^* of the relation R on V may now be viewed as the set of ordered pairs (u, v) such that there is a path from u to v in the graph G. Accordingly, the path matrix P of $G = G(V, R)$ is precisely the adjacency matrix of the graph $G' = G'(V, R^*)$ which corresponds to the transitive closure R^*. Furthermore, by the above discussion, we need only look at simple paths of length $m - 1$ or less and cycles of length m or less. Accordingly, we have the following result which characterizes the transitive closure R^* of R.

Theorem 9.7: Let R be a relation on a set V with m elements. Then:
(i) $R^* = R \cup R^2 \cup \cdots \cup R^m$ is the transitive closure of R.
(ii) The path matrix P of $G(V, R)$ is the adjacency matrix of $G'(V, R^*)$.

9.6 WARSHALL'S ALGORITHM; SHORTEST PATHS

Let G be a directed graph with m vertices, $v_1, v_2, \ldots, v_m$. Suppose we want to find the path matrix P of the graph G. Warshall gave an algorithm which is much more efficient than calculating the powers of the adjacency matrix A. This algorithm is defined in this section, and a similar algorithm is used to find shortest paths in G when G is weighted.

Warshall's Algorithm

First we define m-square Boolean matrices $P_0, P_1, \ldots, P_m$ as follows. Let $P_k[i,j]$ denote the ij entry of the matrix P_k. Then we define:

$$P_k[i,j] = \begin{cases} 1 & \text{if there is a simple path from } v_i \text{ to } v_j \text{ which does not use any other vertices except possibly } v_1, v_2, \ldots, v_k \\ 0 & \text{otherwise} \end{cases}$$

That is,

$P_0[i,j] = 1$ if there is an edge from v_i to v_j

$P_1[i,j] = 1$ if there is a simple path from v_i to v_j which does not use any other vertex except possibly v_1

$P_2[i,j] = 1$ if there is a simple path from v_i to v_j which does not use any other vertices except possibly v_1 and v_2

And so on.

Observe that the first matrix $P_0 = A$, the adjacency matrix of G. Furthermore, since G has only m vertices, the last matrix $P_m = P$, the path matrix of G.

Warshall observed that $P_k[i,j] = 1$ can occur only if one of the following two cases occurs:

(1) There is a simple path from v_i to v_j which does not use any other vertices except possibly v_1, $v_2, \ldots, v_{k-1}$; hence

$$P_{k-1}[i,j] = 1$$

(2) There is a simple path from v_i to v_k and a simple path from v_k to v_j where each simple path does not use any other vertices except possibly $v_1, v_2, \ldots, v_{k-1}$; hence

$$P_{k-1}[i,k] = 1 \qquad \text{and} \qquad P_{k-1}[k,j] = 1$$

These two cases are pictured as follows:

$$(1) \quad v_i \to \cdots \to v_j; \qquad (2) \quad v_i \to \cdots \to v_k \to \cdots \to v_j$$

Here

$$\to \cdots \to$$

denotes part of a simple path which does not use any other vertices except possibly $v_1, v_2, \ldots, v_{k-1}$. Accordingly, the elements of P_k can be obtained by

$$P_k[i,j] \;=\; P_{k-1}[i,j] \;\vee\; (P_{k-1}[i,k] \wedge P_{k-1}[k,j])$$

where we use the logical operations of $\wedge$ (AND) and $\vee$ (OR). In other words we can obtain each entry in the matrix P_k by looking at only three entries in the matrix P_{k-1}. Warshall's algorithm follows.

Algorithm 9.6 (Warshall's Algorithm): A directed graph G with M vertices is maintained in memory by its adjacency matrix A. This algorithm finds the (Boolean) path matrix P of the graph G.

Step 1. Repeat for $I, J = 1, 2, \ldots, M$: [Initializes P.]
If $A[I,J] = 0$, then: Set $P[I,J]: = 0$;
Else: Set $P[I,J]: = 1$.
[End of loop.]

Step 2. Repeat Steps 3 and 4 for $K = 1, 2, \ldots, M$: [Updates P.]

Step 3. Repeat Step 4 for $I = 1, 2, \ldots, M$:

Step 4. Repeat for $J = 1, 2, \ldots, M$:
Set $P[I,J]:= P[I,J] \vee (P[I,K] \wedge P[K,J])$.
[End of loop.]
[End of Step 3 loop.]
[End of Step 2 loop.]

Step 5. Exit.

Shortest-path Algorithm

Let G be a simple directed graph with m vertices, $v_1, v_2, \ldots, v_m$. Suppose G is weighted; that is, suppose each edge e of G is assigned a nonnegative number $w(e)$ called the *weight* or *length* of e. Then G may be maintained in memory by its *weight matrix* $W = (w_{ij})$ defined by

$$w_{ij} = \begin{cases} w(e) & \text{if there is an edge } e \text{ from } v_i \text{ to } v_j \\ 0 & \text{if there is no edge from } v_i \text{ to } v_j \end{cases}$$

The path matrix P tells us whether or not there are paths between the vertices. Now we want to find a matrix Q which tells us the lengths of the shortest paths between the vertices or, more exactly, a matrix $Q = (q_{ij})$ where

$$q_{ij} = \text{length of the shortest path from } v_i \text{ to } v_j$$

Next we describe a modification of Warshall's algorithm which efficiently finds us the matrix Q.

Here we define a sequence of matrices $Q_0, Q_1, \ldots, Q_m$ (analogous to the above matrices $P_0, P_1, \ldots, P_m$) where $Q_k[i,j]$, the ij entry of Q_k, is defined as follows:

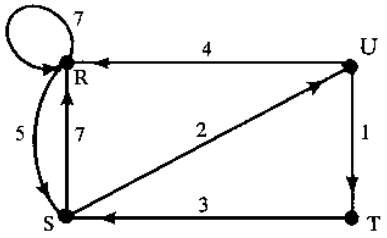
$Q_k[i,j] =$ the smaller of the length of the preceding path from v_i to v_j or the sum of the lengths of the preceding paths from v_i to v_k and from v_k to v_j.

More exactly,

$$Q_k[i,j] \;=\; \text{MIN}\,(Q_{k-1}[i,j],\; Q_{k-1}[i,k] + Q_{k-1}[k,j])$$

The initial matrix Q_0 is the same as the weight matrix W except that each 0 in W is replaced by ∞ (or a very, very large number). The final matrix Q_m will be the desired matrix Q.

EXAMPLE 9.9 Figure 9-9 shows a weighted graph G and its weight matrix W where we assume $v_1 = R$, $v_2 = S$, $v_3 = T$, $v_4 = U$.



$$W = \begin{bmatrix} 7 & 5 & 0 & 0 \\ 7 & 0 & 0 & 2 \\ 0 & 3 & 0 & 0 \\ 4 & 0 & 1 & 0 \end{bmatrix}$$

Fig. 9-9

Suppose we apply the modified Warshall's algorithm to our weighted graph G. We will obtain the matrices Q_0, Q_1, Q_2, Q_3, and Q_4 in Fig. 9-10. (To the right of each matrix Q_k in Fig. 9-10, we show the matrix of paths which correspond to the lengths in the matrix Q_k.) The entries in the matrix Q_0 are the same as the weight matrix W except each 0 in W is replaced by ∞ (a very large number). We indicate how the circled entries are obtained:

$$Q_1[4,2] = \text{MIN}\,(Q_0[4,2], Q_0[4,1] + Q_0[1,2]) = \text{MIN}\,(\infty, 4+5) = 9$$
$$Q_2[1,3] = \text{MIN}\,(Q_1[1,3], Q_1[1,2] + Q_1[2,3]) = \text{MIN}\,(\infty, 5+\infty) = \infty$$
$$Q_3[4,2] = \text{MIN}\,(Q_2[4,2], Q_2[4,3] + Q_2[3,2]) = \text{MIN}\,(9, 3+1) = 4$$
$$Q_4[3,1] = \text{MIN}\,(Q_3[3,1], Q_3[3,4] + Q_3[4,1]) = \text{MIN}\,(10, 5+4) = 9$$

The last matrix $Q_4 = Q$, the desired shortest-path matrix.

$$Q_0 = \begin{pmatrix} 7 & 5 & \infty & \infty \\ 7 & \infty & \infty & 2 \\ \infty & 3 & \infty & \infty \\ 4 & \infty & 1 & \infty \end{pmatrix} \qquad \begin{pmatrix} \text{RR} & \text{RS} & — & — \\ \text{SR} & — & — & \text{SU} \\ — & \text{TS} & — & — \\ \text{UR} & — & \text{UT} & — \end{pmatrix}$$

$$Q_1 = \begin{pmatrix} 7 & 5 & \infty & \infty \\ 7 & 12 & \infty & 2 \\ \infty & 3 & \infty & \infty \\ 4 & \textcircled{9} & 1 & \infty \end{pmatrix} \qquad \begin{pmatrix} \text{RR} & \text{RS} & — & — \\ \text{SR} & \text{SRS} & — & \text{SU} \\ — & \text{TS} & — & — \\ \text{UR} & \text{URS} & \text{UT} & — \end{pmatrix}$$

$$Q_2 = \begin{pmatrix} 7 & 5 & \textcircled{\infty} & 7 \\ 7 & 12 & \infty & 2 \\ 10 & 3 & \infty & 5 \\ 4 & 9 & 1 & 11 \end{pmatrix} \qquad \begin{pmatrix} \text{RR} & \text{RS} & — & \text{RSU} \\ \text{SR} & \text{SRS} & — & \text{SU} \\ \text{TSR} & \text{TS} & — & \text{TSU} \\ \text{UR} & \text{URS} & \text{UT} & \text{URS} \end{pmatrix}$$

$$Q_3 = \begin{pmatrix} 7 & 5 & \infty & 7 \\ 7 & 12 & \infty & 2 \\ 10 & 3 & \infty & 5 \\ 4 & \textcircled{4} & 1 & 6 \end{pmatrix} \qquad \begin{pmatrix} \text{RR} & \text{RS} & — & \text{RSU} \\ \text{SR} & \text{SRS} & — & \text{SU} \\ \text{TSR} & \text{TS} & — & \text{TSU} \\ \text{UR} & \text{UTS} & \text{UT} & \text{UTSU} \end{pmatrix}$$

$$Q_4 = \begin{pmatrix} 7 & 5 & 8 & 7 \\ 7 & 11 & 3 & 2 \\ \textcircled{9} & 3 & 6 & 5 \\ 4 & 4 & 1 & 6 \end{pmatrix} \qquad \begin{pmatrix} \text{RR} & \text{RS} & \text{RSUT} & \text{RSU} \\ \text{SR} & \text{SURS} & \text{SUT} & \text{SU} \\ \text{TSUR} & \text{TS} & \text{TSUT} & \text{TSU} \\ \text{UR} & \text{UTS} & \text{UT} & \text{UTSU} \end{pmatrix}$$

Fig. 9-10

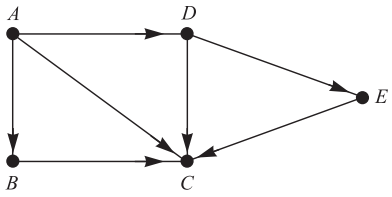
9.7 LINKED REPRESENTATION OF DIRECTED GRAPHS

Let G be a directed graph with m vertices. Suppose the number of edges of G is $O(m)$ or even $O(m \log m)$, that is, suppose G is sparse. Then the adjacency matrix A of G will contain many zeros; hence a great deal of memory space will be wasted. Accordingly, when G is sparse, G is usually represented in memory by some type of *linked representation*, also called an *adjacency structure*, which is described below by means of an example.

Consider the directed graph G in Fig. 9-11(a). Observe that G may be equivalently defined by the table in Fig. 9-11(b), which shows each vertex in G followed by its *adjacency list*, also called its *successors* or *neighbors*. Here the symbol $\varnothing$ denotes an empty list. Observe that each edge of G corresponds to a unique vertex in an adjacency list and vice versa. Here G has seven edges and there are seven vertices in the adjacency lists. This table may also be presented in the compact form

$$G = [A{:}B, C, D; \quad B{:}C; \quad C{:}\varnothing; \quad D{:}C, E; \quad E{:}C]$$

where a colon ":" separates a vertex from its list of neighbors, and a semicolon ";" separates the different lists.



(*a*) Graph G

Vertex	Adjacency list
A	B, C, D
B	C
C	$\varnothing$
D	C, E
E	C

(*b*) Adjacency lists of G

Fig. 9-11

The *linked representation* of a directed graph G maintains G in memory by using linked lists for its adjacency lists. Specifically, the linked representation will normally contain two files (sets of records), one called the Vertex File and the other called the Edge File, as follows.

(*a*) ***Vertex File***: The Vertex File will contain the list of vertices of the graph G usually maintained by an array or by a linked list. Each record of the Vertex File will have the form

VERTEX	NEXT-V	PTR	

Here VERTEX will be the name of the vertex, NEXT-V points to the next vertex in the list of vertices in the Vertex File, and PTR will point to the first element in the adjacency list of the vertex appearing in the Edge File. The shaded area indicates that there may be other information in the record corresponding to the vertex.

(*b*) ***Edge File***: The Edge File contains the edges of G and also contains all the adjacency lists of G where each list is maintained in memory by a linked list. Each record of the Edge File will represent a unique edge in G and hence will correspond to a unique vertex in an adjacency list. The record will usually have the form

EDGE	BEG-V	END-V	NEXT-E	

Here:

(1) EDGE will be the name of the edge (if it has a name).
(2) BEG-V points to location in the Vertex File of the initial (beginning) vertex of the edge.
(3) END-V points to the location in the Vertex File of the terminal (ending) vertex of the edge. The adjacency lists appear in this field.
(4) NEXT-E points to the location in the Edge File of the next vertex in the adjacency list.

We emphasize that the adjacency lists consist of terminal vertices and hence are maintained by the END-V field. The shaded area indicates that there may be other information in the record corresponding to the edge. We note that the order of the vertices in any adjacency list does depend on the order in which the edges (pairs of vertices) appear in the input.

Figure 9-12 shows how the graph G in Fig. 9-11(*a*) may appear in memory. Here the vertices of G are maintained in memory by a linked list using the variable START to point to the first vertex. (Alternatively, one could use a linear array for the list of vertices, and then NEXT-V would not be required.) The choice of eight locations for the Vertex File and 10 locations for the Edge File is arbitrary. The additional space in the files will be used if additional vertices or edges are inserted in the graph. Figure 9-12 also shows, with arrows, the adjacency list $[B, C, D]$ of the vertex A.

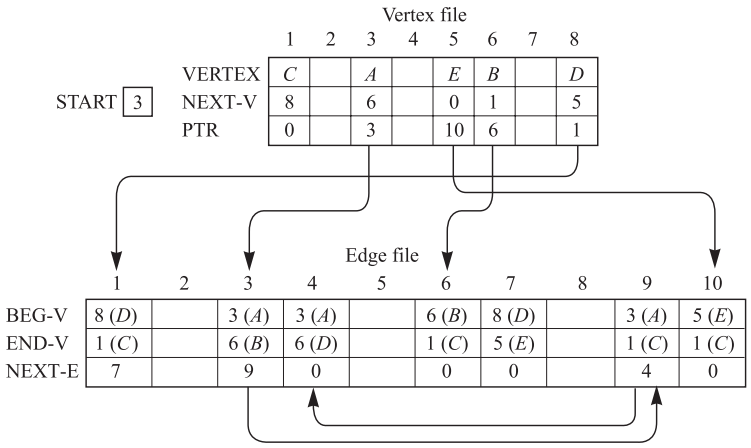

Vertex file
1 2 3 4 5 6 7 8
VERTEX C A E B D
START 3
NEXT-V 8 6 0 1 5
PTR 0 3 10 6 1
Edge file
1 2 3 4 5 6 7 8 9 10
BEG-V 8 (D) 3 (A) 3 (A) 6 (B) 8 (D) 3 (A) 5 (E)
END-V 1 (C) 6 (B) 6 (D) 1 (C) 5 (E) 1 (C) 1 (C)
NEXT-E 7 9 0 0 0 4 0

Fig. 9-12

9.8 GRAPH ALGORITHMS: DEPTH-FIRST AND BREADTH-FIRST SEARCHES

This section discusses two important graph algorithms for a given graph G. Any particular graph algorithm may depend on the way G is maintained in memory. Here we assume G is maintained in memory by its adjacency structure. Our test graph G with its adjacency structure appears in Fig. 9-13.

Many applications of graphs require one to systematically examine the vertices and edges of a graph G. There are two standard ways that this is done. One way is called a *depth-first search* (DFS) and the other is called a *breadth-first search* (BFS). (These algorithms are essentially identical to the analogous algorithms for undirected graph in Chapter 8.)

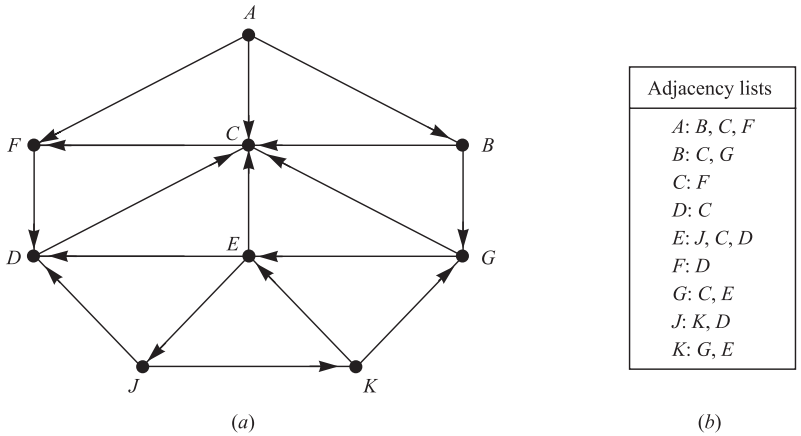


Fig. 9-13

During the execution of our algorithms, each vertex (node) N of G will be in one of three states, called the *status* of N, as follows:

STATUS = 1: (Ready state) The initial state of the vertex N.
STATUS = 2: (Waiting state) The vertex N is on a (waiting) list, waiting to be processed.
STATUS = 3: (Processed state) The vertex N has been processed.

The waiting list for the depth-first search will be a (modified) STACK, whereas the waiting list for the breadth-first search will be a QUEUE.

(*a*) ***Depth-first Search***: The general idea behind a depth-first search beginning at a starting vertex A is as follows. First we process the starting vertex A. Then we process each vertex N along a path P which begins at A; that is, we process a neighbor of A, then a neighbor of a neighbor of A, and so on. After coming to a "dead end", that is, to a vertex with no unprocessed neighbor, we backtrack on the path P until we can continue along another path P'. And so on. The backtracking is accomplished by using a STACK to hold the initial vertices of future possible paths. We also need a field STATUS which tells us the current status of any vertex so that no vertex is processed more than once. The algorithm follows.

Algorithm 9.8A (Depth-first Search): This algorithm executes a depth-first search on a directed graph G beginning with a starting vertex A.

Step 1. Initialize all vertices to the ready state (STATUS = 1).

Step 2. Push the starting vertex A onto STACK and change the status of A to the waiting state (STATUS = 2).

Step 3. Repeat Steps 4 and 5 until STACK is empty.

Step 4. Pop the top vertex N of STACK. Process N, and set STATUS(N) = 3, the processed state.

Step 5. Examine each neighbor J of N.
(*a*) If STATUS (J) = 1 (ready state), push J onto STACK and reset STATUS (J) = 2 (waiting state).
(*b*) If STATUS (J) = 2 (waiting state), delete the previous J from the STACK and push the current J onto STACK.
(*c*) If STATUS (J) = 3 (processed state), ignore the vertex J.
[End of Step 3 loop.]

Step 6. Exit.

The above algorithm will process only those vertices which are reachable from a starting vertex A. Suppose one wants to process all the vertices in the graph G. Then the algorithm must be modified so that it begins again with another vertex that is still in the ready state (STATE = 1). This new vertex, say B, can be obtained by traversing through the list of vertices.

Remark: The structure STACK in the above algorithm is not technically a stack since, in Step 5(*b*), we allow a vertex J to be deleted and then inserted in the front of the stack. (Although it is the same vertex J, it will represent a different edge.) If we do not move J to the top of STACK in Step 5(*b*), then we obtain an alternative traversal algorithm.

EXAMPLE 9.10 Consider our test graph G in Fig. 9-13. Suppose we want to find and print all the vertices reachable from the vertex J (including J itself). One way to do this is to use a depth-first search of G starting at the vertex J.

Applying Algorithm 9.8A, the vertices will be processed and printed in the following order:

$$J, \quad K, \quad G, \quad E, \quad C, \quad F, \quad D$$

Specifically, Fig. 9-14(*a*) shows the sequence of waiting lists in STACK and the vertices being processed. (The

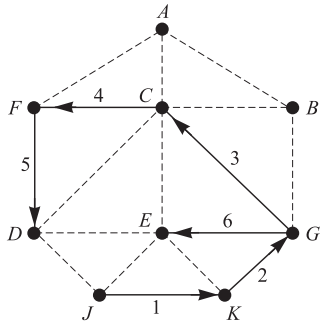
slash / indicates that a vertex is deleted from the waiting list.) We emphasize that each vertex, excluding J, comes from an adjacency list and hence it is the terminal vertex of a unique edge of the graph. We have indicated the edge by prelabeling the terminal vertex with the initial vertex of the edge. For example,

$$J^D$$

means D is in the adjacency list of J, and hence D is the terminal vertex of an edge beginning at J. These edges form a rooted tree T with J as the root, which is pictured in Fig. 9-14(b). (The numbers indicate the order the edges are added to the tree T). This tree T spans the subgraph G' of G consisting of vertices reachable from J.

Vertex	STACK
	J
J	J^K, J^D
J^K	K^G, K^E, J^D
K^G	G^C, G^E, K^E, K^D
G^C	C^F, G^E, K^D
C^F	F^D, G^E, K^D
F^D	G^E
G^E	$\varnothing$

(a)



(b)

Fig. 9-14

(b) ***Breadth-first Search***: The general idea behind a breadth-first search beginning at a starting vertex A is as follows. First we process the starting vertex A. Then we process all the neighbors of A. Then we process all the neighbors of neighbors of A. And so on. Naturally we need to keep track of the neighbors of a vertex, and we need to guarantee that no vertex is processed twice. This is accomplished by using a QUEUE to hold vertices that are waiting to be processed, and by a field STATUS which tells us the current status of a vertex. The algorithm follows.

Algorithm 9.8B (Breadth-first Search): This algorithm executes a breadth-first search on a directed graph G beginning with a starting vertex A.

Step 1. Initialize all vertices to the ready state (STATUS = 1).

Step 2. Put the starting vertex A in QUEUE and change the status of A to the waiting state (STATUS = 2).

Step 3. Repeat Steps 4 and 5 until QUEUE is empty.

Step 4. Remove the first vertex N of QUEUE. Process N, and set STATUS $(N) = 3$, the processed state.

Step 5. Examine each neighbor J of N.
(a) If STATUS $(J) = 1$ (ready state), add J to the rear of QUEUE and reset STATUS $(J) = 2$ (waiting state).
(b) If STATUS $(J) = 2$ (waiting state) or STATUS $(J) = 3$ (processed state), ignore the vertex J.
[End of Step 3 loop.]

Step 6. Exit.

Again, the above algorithm will process only those vertices which are reachable from a starting vertex A. Suppose one wants to process all the vertices in the graph G. Then the algorithm must be modified so that it begins again with another vertex that is still in the ready state (STATE = 1). This new vertex, say B, can be obtained by traversing through the list of vertices.

EXAMPLE 9.11 Consider our test graph G in Fig. 9-13. Suppose G represents the daily flights between cities, and suppose we want to fly from city A to city J with the minimum number of stops. That is, we want to find a shortest path P from A to J (where each edge has weight 1). One way to do this is to use a breadth-first search of G starting at the vertex A, and we stop as soon as J is encountered, that is, added to our waiting list.

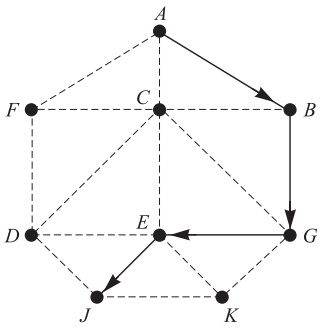
Figure 9-15(a) shows the sequence of waiting lists in QUEUE and the vertices being processed up to the time vertex J is encountered. We then work backwards from J to obtain the desired path

$$E^J \leftarrow G^E \leftarrow B^G \leftarrow A^B \leftarrow A \qquad \text{or} \qquad A \rightarrow B \rightarrow G \rightarrow E \rightarrow J$$

which is pictured in Fig. 9-15(b). Thus a flight from city A to city J will make three intermediate stops, at B, G, and E. Note that the path does not include all of the vertices processed by the algorithm.

Vertex	QUEUE
	A
A	A^B, A^C, A^F
A^F	F^D, A^B, A^C
A^C	F^D, A^B
A^B	B^G, F^D
F^D	B^G
B^G	G^E
G^E	E^J

(a)



(b)

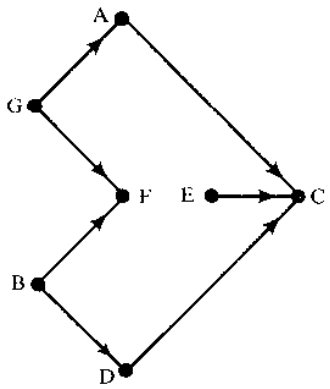
Fig. 9-15

9.9 DIRECTED CYCLE-FREE GRAPHS, TOPOLOGICAL SORT

Let S be a directed graph such that: (1) each vertex v_i of S represents a task, and (2) each (directed) edge (u, v) of S means that the task u must be completed before beginning the task v. Suppose such a graph S contains a cycle, say

$$P = (u, v, w, u)$$

This means we must complete task u before beginning v, we must complete task v before beginning w, and we must complete task w before beginning task u. Thus we cannot begin any of the three tasks in the cycle. Accordingly, such a graph S, representing tasks and a prerequisite relation, cannot have any cycles or, in other words, such a graph S must be *cycle-free* or *acyclic*. A directed acyclic (cycle-free) graph is called a *dag* for short. Figure 9-16 is an example of such a graph.



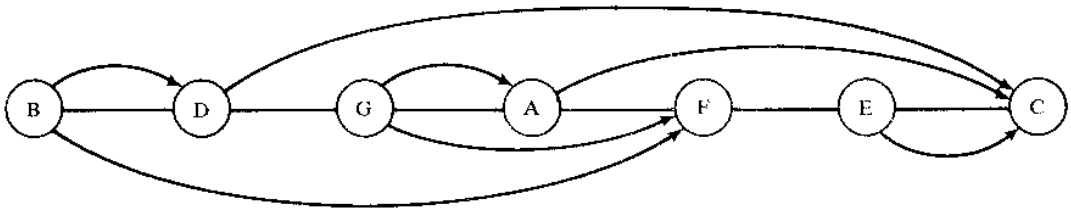
(a)

Adjacency Lists	
A:	C
B:	D, F
C:	
D:	C
E:	C
F:	
G:	A, F

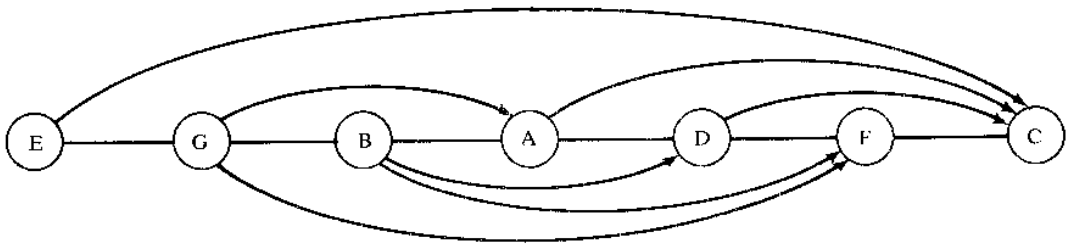
(b)

Fig. 9-16

A fundamental operation on a dag S is to process the vertices one after the other so that the vertex u is always processed before vertex v whenever (u, v) is an edge. Such a linear ordering T of the vertices of S, which may not be unique, is called a *topological sort*. Figure 9-17 shows two topological sorts of the graph S in Fig. 9-16. We have included the edges of S in Fig. 9-17 to show that they agree with the direction of the linear ordering.



(a)



(b)

Fig. 9-17 Two topological sorts.

The following is the main theoretical result in this section.

Theorem 9.8: Let S be a finite directed cycle-free graph. Then there exists a topological sort T of the graph S.

Note that the theorem states only that a topological sort exists. We now give an algorithm which will find a topological sort. The main idea of the algorithm is that any vertex (node) N with zero indegree may be chosen as the first element in the sort T. The algorithm essentially repeats the following two steps until S is empty:

(1) Find a vertex N with zero indegree.
(2) Delete N and its edges from the graph S.

We use an auxiliary QUEUE to temporarily hold all vertices with zero degree. The algorithm follows:

Algorithm 9.9: The algorithm finds a topological sort T of a directed cycle-free graph S.

Step 1. Find the indegree INDEG(N) of each vertex N of S.

Step 2. Insert in QUEUE all vertices with zero degree.

Step 3. Repeat Steps 4 and 5 until QUEUE is empty.

Step 4. Remove and process the front vertex N of QUEUE.

Step 5. Repeat for each neighbor M of the vertex N.
(a) Set INDEG(M) : = INDEG(M) – 1.
[This deletes the edge from N to M.]
(b) If INDEG(M) = 0, add M to QUEUE.
[End of loop.]
[End of Step 3 loop.]

Step 6. Exit.

EXAMPLE 9.12 Suppose Algorithm 9.9 is applied to the graph S in Fig. 9-16. We obtain the following sequence of the elements of QUEUE and sequence of vertices being processed:

Vertex		*B*	*E*	*G*	*D*	*A*	*F*	*C*
QUEUE:	*GEB*	*DGE*	*DG*	*FAD*	*FA*	*CF*	*C*	∅

Figure 9-18 shows that graph S as each of the first three vertices, B, E, and G, and its edges are deleted from S. The topological sort T is the sequence of processed vertices, that is:

$$T: \quad B, E, G, D, A, F, C$$

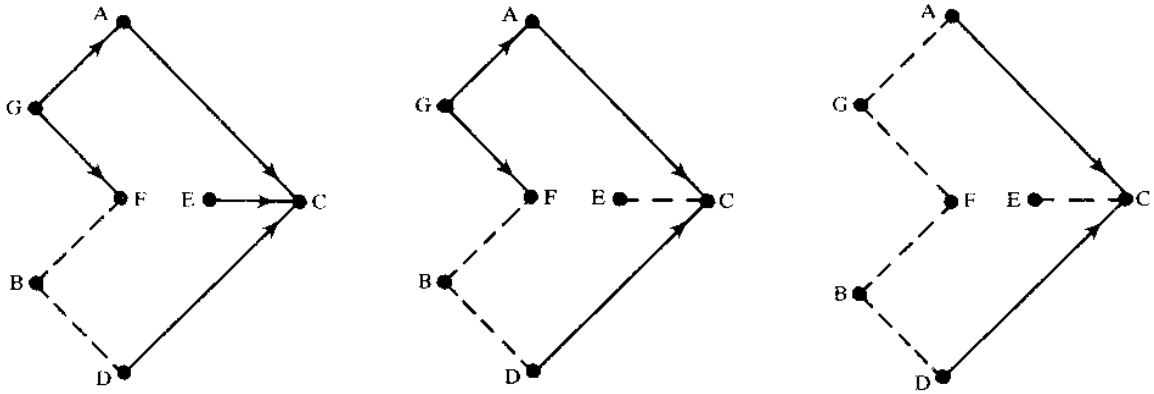


Fig. 9-18

9.10 PRUNING ALGORITHM FOR SHORTEST PATH

Let G be a weighted directed cycle-free graph. We seek the shortest path between two vertices, say, u and w. We assume G is finite so at each step there is a finite number of moves. Since G is cycle-free, all paths between u and w can be given by a rooted tree with u as the root. Figure 9-19(b) enumerates all the paths between u and w in the graph in Fig. 9-19(a).

One way to find the shortest path between u and w is simply to compute the lengths of all the paths of the corresponding rooted tree. On the other hand, suppose two partial paths lead to an intermediate vertex v. From then on, we need only consider the shorter partial path; that is, we prune the tree at the vertex corresponding to the longer partial path. This pruning algorithm is described below.

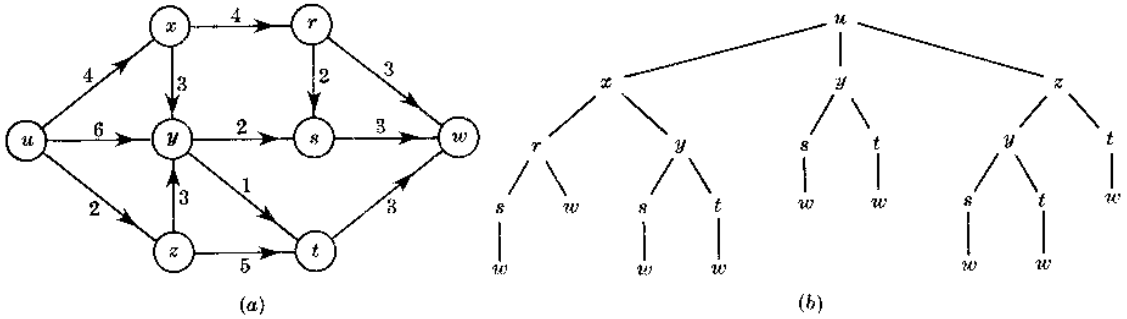


Fig. 9-19

Pruning Algorithm

This algorithm finds the shortest path between a vertex u and a vertex w in a weighted directed cycle-free graph G. The algorithm has the following properties:

(*a*) During the algorithm each vertex v' of G is assigned two things:
  (1) A number $\ell(v')$ denoting the current minimal length of a path from u to v'.
  (2) A path $p(v')$ from u to v' of length $\ell(v')$.

(*b*) Initially, we set $\ell(u) = 0$ and $p(u) = u$. Every other vertex v is initially assigned $\ell(v) = \infty$ and $p(v) = \varnothing$.

(*c*) Each step of the algorithm examines an edge $e = (v', v)$ from v' to v with, say, length k. We calculate $\ell(v') + k$.
  (1) Suppose $\ell(v') + k < \ell(v)$. Then we have found a shorter path from u to v. Thus we update:

$$\ell(v) = \ell(v') + k \qquad \text{and} \qquad p(v) = p(v')v$$

  [This is always true when $\ell(v) = \infty$, that is, when we first enter the vertex v.]
  (2) Otherwise, we do not change $\ell(v)$ and $p(v)$.
  If no other unexamined edges enter v, we will say that $p(v)$ *has been determined.*

(*d*) The algorithm ends when $p(w)$ has been determined.

Remark: The edge $e = (v', v)$ in (*c*) can only be chosen if v' has been previously visited, that is, if $p(v') \neq \varnothing$. Furthermore, it is usually best to examine an edge which begins at a vertex v' whose path $p(v')$ has been determined.

EXAMPLE 9.13 We apply the pruning algorithm to the graph G in Fig. 9-19(*a*).

From u: The successive vertices are x, and z, which are all entered for the first time. Thus:

(1) Set $\ell(x) = 4$, $p(x) = ux$.
(2) Set $\ell(y) = 6$, $p(y) = uy$.
(3) Set $\ell(z) = 2$, $p(z) = uz$.

Note that $p(x)$ and $p(z)$ have been determined.

From x: The successive vertices are r, entered for the first time, and y. Thus:

(1) Set $\ell(r) = 4 + 4 = 8$ and $p(r) = p(x)r = uxr$.
(2) We calculate:

$$\ell(x) + k = 4 + 3 = 7 \text{ which is not less than } \ell(y) = 6.$$

Thus we leave $\ell(y)$ and $p(y)$ alone.
Note that $p(r)$ has been determined.

From z: The successive vertices are t, entered for the first time, and y. Thus:

(1) Set $\ell(t) = \ell(z) + k = 2 + 5 = 7$ and $p(t) = p(z)t = uzt$.
(2) We calculate:

$$\ell(z) + k = 2 + 3 = 5 \text{ which is less than } \ell(y) = 6.$$

We have found a shorter path to y, and so we update $\ell(y)$ and $p(y)$ accordingly, that is, set

$$\ell(y) = \ell(z) + k = 5 \qquad \text{and} \qquad p(y) = p(z)y = uzy$$

Now $p(y)$ has been determined.

From y: The successive vertices are s, entered for the first time, and t. Thus:

(1) Set $\ell(s) = \ell(y) + k = 5 + 2 = 7$ and $p(s) = p(y)s = uzys$.
(2) We calculate:

$$\ell(y) + k = 5 + 1 = 6 \text{ which is less than } \ell(t) = 7.$$

Thus we change $\ell(t)$ and $p(t)$ to read:

$$\ell(t) = \ell(y) + 1 = 6 \qquad \text{and} \qquad p(t) = p(y)t = uzyt.$$

Now $p(t)$ has been determined.

From r: The successive vertices are w, entered for the first time, and s. Thus:

(1) Set $\ell(w) = \ell(r) + 3 = 11$ and $p(w) = p(r)w = uxrw$.
(2) We calculate:

$$\ell(r) + k = 8 + 2 = 10 \text{ which is not less than } \ell(s) = 7.$$

Thus we leave $\ell(s)$ and $p(s)$ alone.
Note that $p(s)$ has been determined.

From s: The successive vertex is w. We calculate:

$$\ell(s) + k = 7 + 3 = 10 \text{ which is less than } \ell(w) = 11.$$

Thus we change $\ell(w)$ and $p(w)$ to read:

$$\ell(w) = \ell(s) + 3 = 10 \qquad \text{and} \qquad p(w) = p(s)w = uzysw.$$

From t: The successive vertex is w. We calculate:

$$\ell(t) + k = 6 + 3 = 9 \text{ which is less than } \ell(w) = 10.$$

Thus we change $\ell(w)$ and $p(w)$ to read:

$$\ell(w) = \ell(t) + 3 = 9 \qquad \text{and} \qquad p(w) = p(t)w = uzytw$$

Now $p(w)$ has been determined.

The algorithm is finished since $p(w)$ has been determined. Thus:

$$p(w) = uzytw$$

is the shortest path from u to w and $\ell(w) = 9$.

The edges which were examined in the above example form the rooted tree in Fig. 9-20. This is the tree in Fig. 9-19(*b*) which has been pruned at vertices belonging to longer partial paths. Observe that only 13 of the original 23 edges of the tree had to be examined.

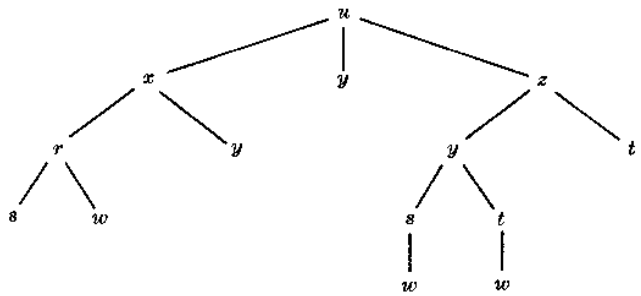


Fig. 9-20

Solved Problems

GRAPH TERMINOLOGY

9.1. Consider the directed graph G in Fig. 9-21.

(a) Describe G formally.

(b) Find all simple paths from X to Z.

(c) Find all simple paths from Y to Z.

(d) Find all cycles in G.

(e) Is G unilaterally connected? Strongly connected?

(a) The vertex set V has four vertices and the edge set E has seven (directed) edges as follows:

$$V = \{X, Y, Z, W\} \qquad \text{and} \qquad E = \{(X, Y), (X, Z), (X, W), (Y, W), (Z, Y), (Z, W), (W, Z)\}$$

(b) There are three simple paths from X to Z, which are (X, Z), (X, W, Z), and (X, Y, W, Z).

(c) There is only one simple path from Y to Z, which is (Y, W, Z).

(d) There is only one cycle in G, which is (Y, W, Z, Y)

(e) G is unilaterally connected since (X, Y, W, Z) is a spanning path. G is not strongly connected since there is no closed spanning path.

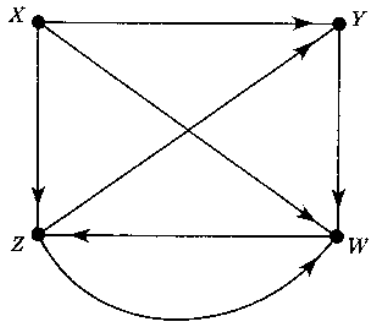


Fig. 9-21

9.2. Consider the directed graph G in Fig. 9-21.

(a) Find the indegree and outdegree of each vertex of G.

(b) Find the successor list of each vertex of G.

(c) Are there any sources or sinks?

(d) Find the subgraph H of G determined by the vertex set $V' = \{X, Y, Z\}$.

(a) Count the number of edges ending and beginning at a vertex v to obtain, respectively, $\text{indeg}(v)$ and $\text{outdeg}(v)$. This yields the data:

$$\begin{aligned} &\text{indeg}(X) = 0, \quad &&\text{indeg}(Y) = 2, \quad &&\text{indeg}(Z) = 2, \quad &&\text{indeg}(W) = 3 \\ &\text{outdeg}(X) = 3, \quad &&\text{outdeg}(Y) = 1, \quad &&\text{outdeg}(Z) = 2, \quad &&\text{outdeg}(W) = 1 \end{aligned}$$

(As expected, the sum of the indegrees and the sum of the outdegrees each equal 7, the number of edges.)

(b) Add vertex v to the successor list $\text{succ}(u)$ of u for each edge (u, v) in G. This yields:

$$\text{succ}(X) = [Y, Z, W], \quad \text{succ}(Y) = [W], \quad \text{succ}(Z) = [Y, W], \quad \text{succ}(W) = [Z]$$

(*c*) X is a source since no edge enters X, that is, indeg $(X) = 0$. There are no sinks since every vertex is the initial point of an edge, that is, has a nonzero outdegree.

(*d*) Let E' consists of all edges of G whose endpoints lie in V'. This yields $E' = \{(X, Y), (X, Z), (Z, Y)\}$. Then $H = H(V', E')$.

9.3. Consider the directed graph in Fig. 9-22.

(*a*) Find two simple paths from v_1 to v_6. Is

$$\alpha = (v_1, v_2, v_4, v_6) \text{ such a simple path?}$$

(*b*) Find all cycles in G which include v_3.

(*c*) Is G unilaterally connected? Strongly connected?

(*a*) A simple path is a path where all vertices are distinct. Thus (v_1, v_5, v_6) and $(v_1, v_2, v_3, v_5, v_6)$ are two simple path from v_1 to v_6. The sequence α is not even a path since the edge joining v_4 to v_6 does not begin at v_4.

(*b*) There are two such cycles: (v_3, v_1, v_2, v_3) and $(v_3, v_5, v_6, v_1, v_2, v_3)$.

(*c*) G is unilaterally connected since $(v_1, v_2, v_3, v_5, v_6, v_4)$ is a spanning path. G is not strongly connected since there is no closed spanning path.

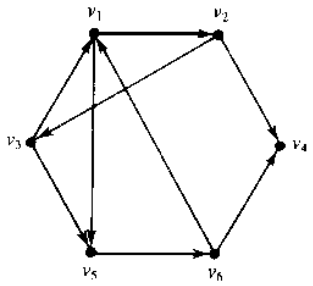


Fig. 9-22

9.4. Consider the directed graph in Fig. 9-22.

(*a*) Find the successor list of each vertex of G.

(*b*) Are there any sources in G? Any sinks?

(*a*) Add vertex v to the successor list succ (u) of u for each edge (u, v) in G. This yields:

$$\begin{aligned} &\text{succ}\,(v_1) = [v_2, v_5], \quad &&\text{succ}\,(v_2) = [v_3, v_4], \quad &&\text{succ}\,(v_3) = [v_1, v_5] \\ &\text{succ}\,(v_4) = \varnothing, \quad &&\text{succ}\,(v_5) = [v_6], \quad &&\text{succ}\,(v_6) = [v_1, v_4] \end{aligned}$$

(As expected, the number of successors equals 9, which is the number of edges.)

(*b*) There are no sources since every vertex is the endpoint of some edge. Only v_4 is a sink since no edge begins at v_4, that is, succ $(v_4) = \varnothing$, the empty set.

9.5. Consider the following directed graph G:

$$V(G) = \{a, b, c, d, e, f, g\}$$

$$E(G) = \{(a, a), (b, e), (a, e), (e, b), (g, c), (a, e), (d, f), (d, b), (g, g)\}$$

(a) Identify any loops or parallel edges.

(b) Are there any sources in G?

(c) Are there any sinks in G?

(d) Find the subgraph H of G determined by the vertex set $V' = \{a, b, c, d\}$.

(a) A loop is an edge with the same initial and terminal points; hence (a, a) and (g, g) are loops. Two edges are parallel if they have the same initial and terminal points. Thus (a, e) and (a, e) are parallel edges.

(b) The vertex d is a source since no edge ends in d, that is, d does not appear as the second element in any edge. There are no other sources.

(c) Both c and f are sinks since no edge begins at c or at f, that is, neither c nor f appear as the first element in any edge. There are no other sinks.

(d) Let E' consist of all edges of G whose endpoints lie in $V' = \{a, b, c, d\}$. This yields $E' = \{(a, a), (d, b)\}$. Then $H = H(V', E')$.

9.6. Let G be the directed graph with vertex set $V(G) = \{a, b, c, d, e\}$ and the following successor lists:

$$\text{succ}\,(a) = [b, c], \qquad \text{succ}\,(b) = \varnothing, \qquad \text{succ}\,(c) = [d, e]$$

$$\text{succ}\,(d) = [a, b, e], \qquad \text{succ}\,(e) = \varnothing$$

(a) List the edges of G. (Thus G is determined by its successor lists.)

(b) Is G weakly connected? Unilaterally connected? Strongly connected?

(a) Draw an edge (x, y) whenever $y \in \text{succ}\,(x)$. This yields:

$$E(G) = \{(a, b), (a, c), (c, d), (c, e), (d, a), (d, b), (d, e)\}$$

(b) Since b and e are sinks, there is no path from b to e or from e to b. Thus G is neither unilaterally nor strongly connected. However, G is weakly connected, since (c, a, b, d, e) is a spanning semipath.

ROOTED TREES, ORDERED ROOTED TREES

9.7. Consider the rooted tree T in Fig. 9-23.

(a) Identify the path α from the root R to each of the following vertices, and find the level number n of the vertex: (i) H; (ii) F; (iii) M.

(b) Find the siblings of E.

(c) Find the leaves of T.

(a) List the vertices while proceeding from R down the tree to the vertex. The number of vertices, other than R, is the level number:
(i) $\alpha = (R, A, C, H)$, $n = 3$; (ii) $\alpha = (R, B, F)$, $n = 2$; (iii) $\alpha = (R, B, G, L, M)$, $n = 4$.

(b) The siblings of E are F and G since they all have the same parent B.

(c) The leaves are vertices with no children, that is, H, D, I, J, K, M, N.

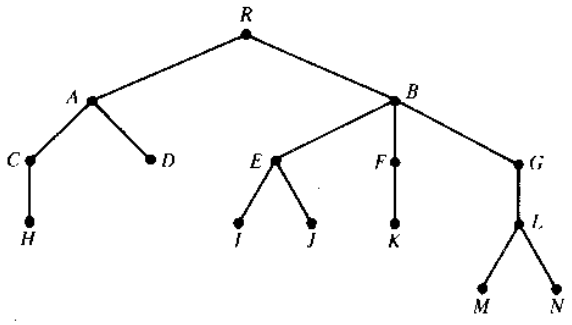


Fig. 9-23

9.8. Consider this typical business situation. A company which sells its products in two major geographic regions is planning to introduce a new product. The normal procedure for product introduction is as follows. First, the product is introduced in a very small test market in region I. If the product fails, it is discontinued; if it succeeds, it is introduced in all of region I. If the product is a success in region I, it is introduced in all of region II; if not, it is introduced in a small test market in region II. Again, if it is successful, it is introduced to the entire region. Use a tree to identify all the possible outcomes of the product introduction procedure.

The possible outcomes are described by the tree in Fig. 9-24. There are four possible outcomes as indicated by the four branches from the root to the leaves of the tree (where now the root is on the left of the tree):

(1) The product is not successful in the first small market test of region I and is discontinued.
(2) The product is successful in the first small test market, is successful in region I, and is introduced in region II.
(3) The product is successful in the first small test market but is not successful in region I. It is tested in the small test market in region II, is not successful, and is discontinued.
(4) The product is successful in the first small test market but is not successful in region I. It is tested in a small test market in region II, is successful, and is introduced to that region.

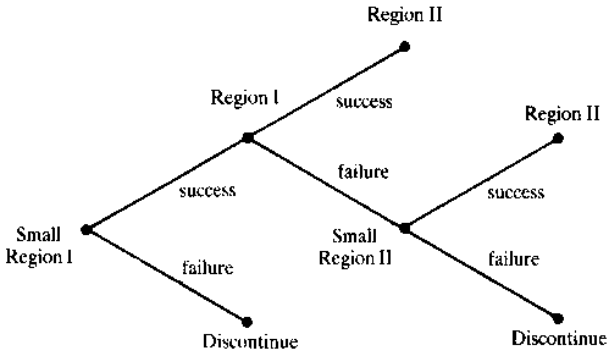


Fig. 9-24

9.9. Figure 9-25 shows an ordered rooted tree T whose vertices are labeled using the universal address system. Find the lexicographic order of the addresses of the tree T.

Since an ordered rooted tree T is usually drawn so that the edges are ordered from left to right as in Fig. 9-25, the lexicographic order can be obtained by reading down the leftmost branch, then the second branch from the left, and so forth. Accordingly, reading down the leftmost branch of T we obtain:

0, 1, 1.1, 1.1.1

The next branch is 1.2, so we add 1.2 to the list to obtain

0, 1, 1.1, 1.1.1, 1.2

Similarly, the next branch adds

1.3, 1.3.1, 1.3.1.1

to our list. Proceeding in this manner, we obtain

0, 1, 1.1, 1.1.1, 1.2, 1.3, 1.3.1, 1.3.1.1, 1.3.2, 2, 2.1, 2.2, 2.2.1.

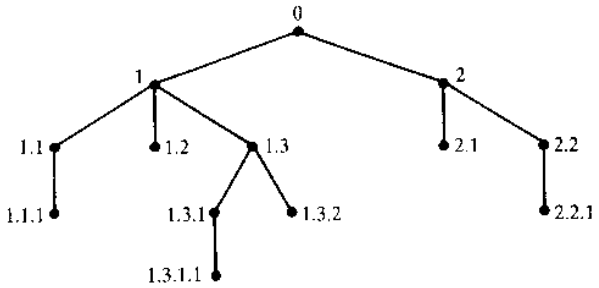


Fig. 9-25

9.10. Consider the following addresses which are in random order:

1, 2.2.1, 3.2, 2.2.1.1, 1.1.1, 0, 2.1, 3.2.1.1,
3, 3.1, 2.2, 2.1.1, 3.2.1, 1.1, 3.2.1.2, 2, 1.1.2

(*a*) Place the addresses in lexicographic order.

(*b*) Draw the corresponding ordered rooted tree.

(*a*) The lexicographic order of the addresses is as follows:

0, 1, 1.1, 1.1.1, 1.1.2, 2, 2.1, 2.1.1, 2.2, 2.2.1,
2.2.1.1, 3, 3.1, 3.2 3.2.1, 3.2.1.1, 3.2.1.2

(*b*) To draw the tree T associated with the given lexicographic order, start with the leftmost branch, then add the branch next to it, and so forth. Thus draw the root 0 branching to 1, branching to 1.1, and then branching to 1.1.1. Since 2 does not succeed 1.1.1 in the tree, this is the beginning of the next branch, which is 2, 2.1, 2.1.1. Continuing in this manner yields the tree in Fig. 9-26.

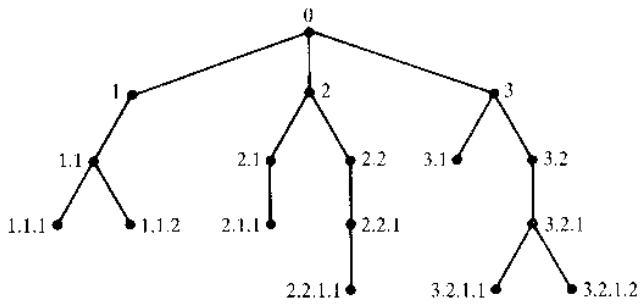


Fig. 9-26

SEQUENTIAL REPRESENTATION OF GRAPHS

9.11. Consider the graph G in Fig. 9-21. Suppose the vertices are stored in memory in an array DATA as follows:

$$\text{DATA: } X,\ Y,\ Z,\ W$$

(*a*) Find the adjacency matrix A of the graph G.

(*b*) Find the path matrix P of G using powers of the adjacency matrix A.

(*c*) Is G strongly connected?

(*a*) The vertices (nodes) are normally ordered according to the way they appear in memory; that is, we assume $v_1 = X$, $v_2 = Y$, $v_3 = Z$, $v_4 = W$. The adjacency matrix A of G follows:

$$A = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Here $a_{ij} = 1$ if there is an edge from v_i to v_j; otherwise, $a_{ij} = 0$.

(*b*) Since G has four vertices, compute A^2, A^3, A^4, and $B_4 = A + A^2 + A^3 + A^4$:

$$A^2 = \begin{pmatrix} 0 & 1 & 1 & 2 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}, \qquad A^3 = \begin{pmatrix} 0 & 1 & 2 & 2 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

$$A^4 = \begin{pmatrix} 0 & 2 & 2 & 3 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \\ 0 & 1 & 1 & 1 \end{pmatrix}, \qquad B_4 = \begin{pmatrix} 0 & 5 & 6 & 8 \\ 0 & 1 & 2 & 3 \\ 0 & 3 & 3 & 5 \\ 0 & 2 & 3 & 5 \end{pmatrix}$$

The path matrix P is now obtained by setting $p_{ij} = 1$ wherever there is a nonzero entry in the matrix B_4. Thus

$$P = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}$$

(*c*) The path matrix shows that there is no path from v_2 to v_1. In fact, there is no path from any node to v_1. Thus G is not strongly connected.

9.12. Consider the adjacency matrix A of the graph G in Fig. 9-21 obtained in Problem 9.11. Find the path matrix P of G using Warshall's algorithm rather than the powers of A.

Compute the matrices P_0, P_1, P_2, P_3 and P_4 where initially $P_0 = A$ and

$$P_k[i,j] = P_{k-1}[i,j] \vee (P_{k-1}[i,j] \wedge P_{k-1}[k,j])$$

That is,

$$P_k[i,j] = 1 \quad \text{if} \quad P_{k-1}[i,j] = 1 \quad \text{or both} \quad P_{k-1}[i,k] = 1 \quad \text{and} \quad P_{k-1}[k,j] = 1$$

Then:

$$P_1 = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \qquad P_2 = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$P_3 = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}, \qquad P_4 = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}$$

Observe that $P_0 = P_1 = P_2 = A$. The changes in P_3, occur for the following reasons:

$$P_3(4,2) = 1 \quad \text{because} \quad P_2(4,3) = 1 \quad \text{and} \quad P_2(3,2) = 1$$
$$P_3(4,4) = 1 \quad \text{because} \quad P_2(4,3) = 1 \quad \text{and} \quad P_2(3,4) = 1$$

The changes in P_4 occur similarly. The last matrix, P_4, is the required path matrix P of the graph G.

9.13. Draw a picture of the weighted graph G which is maintained in memory by the following vertex array DATA and weight matrix W:

$$\text{DATA: } X,\ Y,\ S,\ T; \qquad W = \begin{bmatrix} 0 & 0 & 3 & 0 \\ 5 & 0 & 1 & 7 \\ 2 & 0 & 0 & 4 \\ 0 & 6 & 8 & 0 \end{bmatrix}$$

The picture appears in Fig. 9-27. The vertices are labeled by the entries in DATA. Also, if $w_{ij} \neq 0$, then there is an edge from v_i to v_j with weight w_{ij}. (We assume $v_1 = X$, $v_2 = Y$, $v_3 = S$, $v_4 = T$, the order in which the vertices appear in the array DATA.)

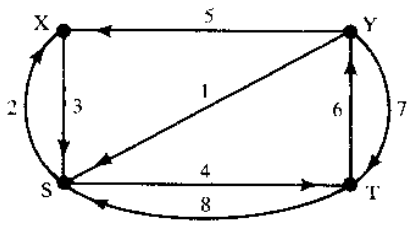


Fig. 9-27

9.14. Prove Proposition 9.4: Let A be the adjacency matrix of a graph G. Then $a_K(i,j)$, the ij entry in the matrix A^K, gives the number of paths of length K from v_i to v_j.

The proof is by induction on K. Note first that a path of length 1 from v_i to v_j is precisely an edge (v_i, v_j). By definition of the adjacency matrix A, $a_i(i,j) = a_{ij}$ gives the number of edges from v_i to v_j. Hence the proposition is true for $K = 1$.

Suppose $K > 1$. (Assume G has m nodes.) Since $A^K = A^{K-1}A$,

$$a_K(i,j) = \sum_{s=1}^{m} a_{K-1}(i,s)a_1(s,j)$$

By induction, $a_{K-1}(i,s)$ gives the number of paths of length $K-1$ from v_1 to v_s, and $a_1(s,j)$ gives the number of paths of length 1 from v_s to v_j. Thus $a_{K-1}(i,s)a_1(s,j)$ gives the number of paths of length K from v_i to v_j where v_s is the next-to-last node. Thus all the paths of length K from v_i to v_j can be obtained by summing up the $a_{K-1}(i,s)a_1(s,j)$ for all s. That is, $a_K(i,j)$ is the number of paths of length K from v_i to v_j. Thus the proposition is proved.

LINKED REPRESENTATION OF GRAPHS

9.15. A weighted graph G with six vertices, $A, B, \ldots, F$, is stored in memory using a linked representation with a vertex file and an edge file as in Fig. 9-28.

(*a*) List the vertices in the order they appear in memory.

(*b*) Find the successor list succ (v) of each vertex v.

Vertex file

START 3

	1	2	3	4	5	6	7	8
VERTEX	*D*		*B*	*F*	*A*		*C*	*E*
NEXT-V	7		1	5	0		8	4
PTR	9		3	0	6		10	1

Edge file

	1	2	3	4	5	6	7	8	9	10
BEG-V	8	5	3		5	5	3		1	7
END-V	1	4	7		3	1	1		8	8
NEXT-E	0	5	7		0	2	0		0	0
WEIGHT	3	4	2		6	3	1		2	5

Fig. 9-28

(*a*) Since START = 3, the list begins with the vertex B. Then NEXT-V tells us to go to $1(D)$, then $7(C)$, then $8(E)$, then $4(F)$, and then $5(A)$; that is,

$$B, \quad D, \quad C, \quad E, \quad F, \quad A$$

(*b*) Here succ $(A) = [1(D), 4(F), 3(B)] = [D, F, B]$. Specifically, PTR$[5(A)] = 6$ and END-V$[6] = 1(D)$ tells us that succ (A) begins with D. Then NEXT-E$[6] = 2$ and END-V$[2] = 4(F)$ tells us that F is the next vertex in succ (A). Then NEXT-E$[2] = 5$ and END-V$[5] = 3(B)$ tells us that B is the next vertex in succ (A). However, NEXT-E$[5] = 0$ tells us that there are no more successors of A. Similarly,

$$\text{succ}\,(B) = [C, D], \qquad \text{succ}\,(C) = [E], \qquad \text{succ}\,(D) = E, \qquad \text{succ}\,(E) = [D]$$

Furthermore succ $(F) = \varnothing$, since PTR$[4(F)] = 0$. In other words,

$$G \quad = \quad [A{:}D, F, B; \quad B{:}C, D; \quad C{:}E; \quad D{:}E; \quad E{:}D; \quad F{:}\varnothing]$$

9.16. Consider the weighted graph G whose linked representation appears in Fig. 9-28. Draw the graph of G.

Use the successor lists obtained in Problem 9.16(*b*) and the weights of the edges in the Edge File in Fig. 9-28 to draw the graph of G in Fig. 9-29.

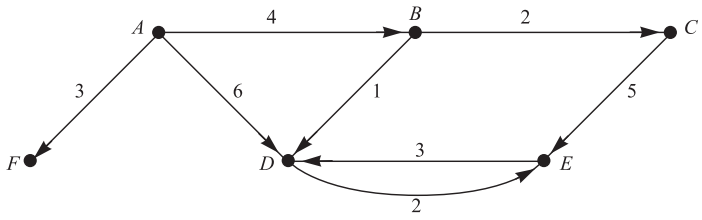


Fig. 9-29

9.17. Suppose a graph G is presented by the following table:

$$G = [X{:}Y, Z, W; \quad Y{:}X, Y, W; \quad Z{:}Z, W; \quad W{:}Z]$$

(*a*) Find the number of vertices and edges in G.

(*b*) Are there any sources or sinks?

(*c*) Draw the graph of G.

(*a*) The table tells us that there are four vertices, X, Y, Z, W, and that the outdegrees of the vertices are 3, 3, 2, and 1, respectively. Thus there are $3 + 3 + 2 + 1 = 9$ edges.

(*b*) No vertex has zero outdegrees, so there are no sinks. Also, each vertex is a successor, hence there are no sources.

(*c*) Using the adjacency lists, draw the graph G in Fig. 9-30.

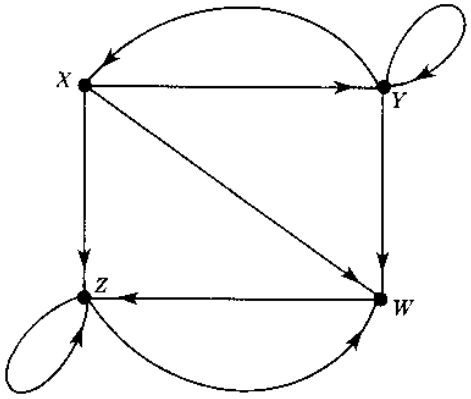


Fig. 9-30

9.18. Suppose Friendly Airways has nine daily flights as follows:

103	Atlanta to Houston	203	Boston to Denver	305	Chicago to Miami
106	Houston to Atlanta	204	Denver to Boston	308	Miami to Boston
201	Boston to Chicago	301	Denver to Reno	401	Reno to Chicago

Describe the data by means of a labeled directed graph G.

The data are described by the graph G in Fig. 9-31 (where the flight numbers have been omitted for notational convenience).

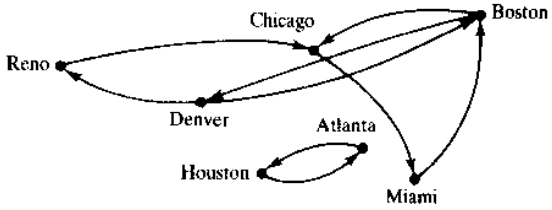


Fig. 9-31

9.19. Describe how the graph G in Problem 9.18 may appear in memory using a linked representation where the cities and flights appear in linear sorted arrays.

See Fig. 9-32 (where A, B, ... denote, respectively, Atlanta, Boston, ...). Note that there is no need for a START variable since the cities form an array, not a linked list. We have also used ORIG (origin) and DEST (destination) instead of BEG-V and END-V.

Vertex file

	1	2	3	4	5	6	7	8
CITY	*A*	*B*	*C*	*D*	*H*	*M*	*R*	
PTR	1	3	7	5	2	8	9	

Edge file

	1	2	3	4	5	6	7	8	9	10
NUMBER	103	106	201	203	204	301	305	308	402	
ORIG	1	5	2	2	4	4	3	6	7	
DEST	5	1	3	4	2	7	6	2	3	
NEXT-E	0	0	4	0	6	0	0	0	0	

Fig. 9-32

9.20. Clearly, the data in Problem 9.18 may be efficiently stored in a file where each record contains only three fields:

Flight Number, City of Origin, City of Destination

However, when there are many, many flights, such a representation does not easily answer the following natural questions:

(i) Is there a direct flight from city X to city Y?

(ii) Can one fly from city X to city Y?

(iii) What is the most direct route (minimum number of stops) from city X to city Y?

Show how the answer, say, to (ii) may be more readily available if the data is stored in memory using the linked representation of a graph as in Fig. 9-32.

One way to answer (ii) is to use a breadth-first or depth-first search algorithm to decide whether city Y is reachable from city X. Such algorithms require the adjacency lists, which can easily be obtained from the linked representation of a graph, but not from the above representation which uses only three fields.

MISCELLANEOUS PROBLEMS

9.21. Draw the multigraph G corresponding to the following adjacency matrix A which has non-negative integer entries:

$$A = \begin{bmatrix} 0 & 2 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 2 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

Since A is a 4×4 matrix, G has four vertices, say, v_1, v_2, v_3, v_4. For each entry a_{ij} draw a_{ij} arcs (directed edges) from vertex v_1 to vertex v_j to obtain the graph in Fig. 9-33.

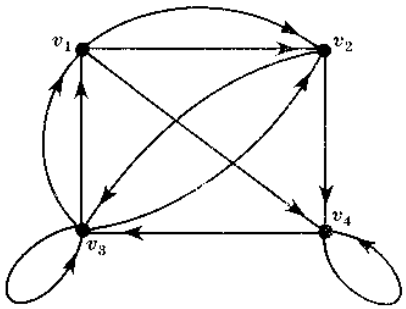


Fig. 9-33

9.22. Consider the cycle-free directed graph S in Fig. 9-34. Find all possible topological sorts of S.

There are four possible topological sorts of S. Specifically, each sort T must begin with either a or b, must end with e or f, and c and d must be the third and fourth elements, respectively. The four sorts follow:

$$T_1 = [a, b, c, d, e, f], \qquad T_2 = [b, a, c, d, e, f]$$
$$T_3 = [a, b, c, d, f, e], \qquad T_4 = [b, a, c, d, f, e]$$

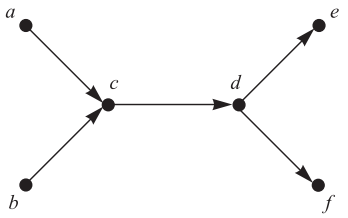


Fig. 9-34

Supplementary Problems

GRAPH TERMINOLOGY

9.23. Consider the graph G in Fig. 9-35.

(*a*) Find the indegree and outdegree of each vertex.
(*b*) Are there any sources or sinks?
(*c*) Find all simple paths from v_1 to v_4.
(*d*) Find all cycles in G.
(*e*) Find all paths of length 3 or less from v_1 to v_3.
(*f*) Is G unilaterally connected? Strongly connected?

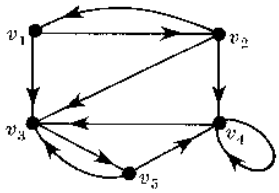


Fig. 9-35

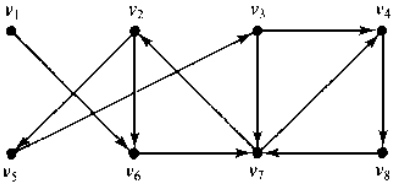


Fig. 9-36

9.24. Consider the graph G in Fig. 9-36.

(*a*) Are there any sources or sinks?
(*b*) Find all simple paths from v_1 to v_4.
(*c*) Find a nonsimple path from v_1 to v_4.
(*d*) Find all cycles in G which include v_4.

9.25. Consider the graph G in Fig. 9-36.

(*a*) Find succ (v_1), succ (v_3), succ (v_5), succ (v_7).
(*b*) Find the subgraph H of G generated by: (i) $\{v_1, v_3, v_5, v_6\}$; (ii) $\{v_2, v_3, v_6, v_7\}$.

9.26. Consider the graph G where

$$V(G) = \{A, B, C, D, E\} \text{ and } E(G) = \{(A, D), (B, C), (C, E), (D, B), (D, D), (D, E), (E, A)\}$$

(*a*) Express G by its adjacency table.
(*b*) Does G have any loops or parallel edges?
(*c*) Find all simple paths from D to E.
(*d*) Find all cycles in G.
(*e*) Is G unilaterally connected? Strongly connected?
(*f*) Find the number of subgraphs of G with vertices C, D, E.
(*g*) Find the subgraph H of G generated by C, D, E.

9.27. Consider the graph in Fig. 9-37.

(*a*) Express G by its adjacency table.
(*b*) Does G have any sources or sinks?
(*c*) Find all simple paths from A to E.
(*d*) Find all cycles in G.

(*e*) Show that G is unilaterally connected by exhibiting a spanning path of G.

(*f*) Is G strongly connected?

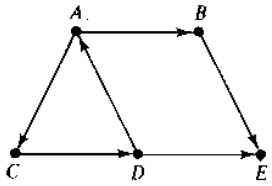


Fig. 9-37

9.28. Draw a labeled graph G that represents the following situation. Three sisters, Barbara, Rose, and Susan, each regularly telephone their mother Gertrude, though Gertrude calls only Rose. Susan will not call Rose, though Rose continues to call Susan. Barbara and Susan will call each other, as will Barbara and Rose.

9.29. Let R be the relation (directed graph) on $V = \{2, 3, 4, 9, 15\}$ defined by "x is less than and relatively prime to y". (*a*) Draw the diagram of the graph R. (*b*) Is R weakly connected? Unilaterally connected? Strongly connected?

9.30. A directed graph G is *complete* if, for each pair of distinct vertices u and v, either (u, v) is an arc or (v, u) is an arc. Show that a finite complete directed graph G has a path which includes all vertices. (This obviously holds for nondirected complete graphs.) Thus G is unilaterally connected.

ROOTED TREES, ORDERED ROOTED TREES

9.31. Consider the rooted tree T in Fig. 9-38.

(*a*) Identify the path α from the root R to each of the following vertices, and find the level number of the vertex: (i) D; (ii) J; (iii) G.

(*b*) Find the leaves of T.

(*c*) Assuming T is an ordered rooted tree, find the universal address of each leaf of T.

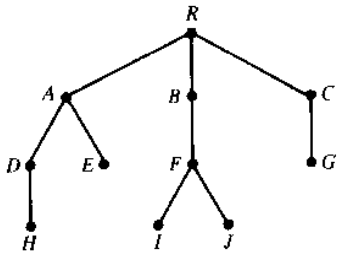


Fig. 9-38

9.32. The following addresses are in random order:

2.1.1, 3.1, 2.1, 1, 2.2.1.2, 0, 3.2, 2.2, 1.1, 2, 3.1.1, 2.2.1, 3, 2.2.1.1

(*a*) Place the addresses in lexicographic order.

(*b*) Draw the corresponding rooted tree.

9.33. Consider the algebraic expression $E = \dfrac{(3x - 5z)^4}{a(2b + c^2)}$.

(*a*) Draw the corresponding ordered rooted tree T, using an arrow ($\uparrow$) for exponentiation, an asterisk ($*$) for multiplication, and a slash ($/$) for division.

(*b*) Use T to rewrite E in Polish prefix form.

SEQUENTIAL REPRESENTATION OF GRAPHS

9.34. Consider the graph G in Fig. 9-39.

(*a*) Find the adjacency matrix A and the path matrix P for G.

(*b*) Find n_k for all $k > 0$ where n_k denotes the number of paths of length k from v_1 to v_4.

(*c*) Is G weakly connected? Unilaterally connected? Strongly connected?

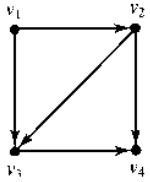


Fig. 9-39

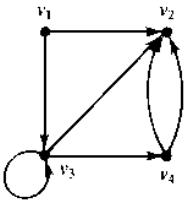


Fig. 9-40

9.35. Repeat Problem 9.34 for the graph in Fig. 9-40.

9.36. Let P be the path matrix for a graph G. Describe P when: (*a*) G is strongly connected; (*b*) G is unilaterally connected.

9.37. Consider the graph G in Fig. 9-41 where, say, the array DATA: X, Y, Z, S, T maintains the vertices in memory.

(*a*) Find the adjacency matrix A and the path matrix P of G.

(*b*) Find all cycles in G.

(*c*) Is G unilaterally connected? Strongly connected?

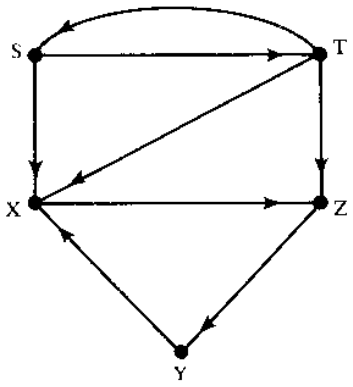


Fig. 9-41

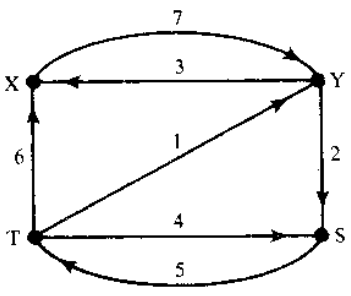


Fig. 9-42

9.38. Consider the weighted graph G in Fig. 9-42 where, say, the array DATA: X, Y, S, T maintains the vertices in memory.

(*a*) Find the weight matrix W of G.

(*b*) Find the matrix Q of shortest paths using Warshall's algorithm.

9.39. Suppose a graph G is input by means of an integer M, representing the vertices 1, 2, ..., M, and a list of N ordered pairs of integers representing the edges of G. Write a procedure for each of the following:

(*a*) To find the $M \times M$ adjacency matrix A of the graph G.

(*b*) To use A and Warshall's algorithm to find the path matrix P of G.

Test the above using the following data:

(i) $M = 5$; $N = 8$; (3,4), (5,3), (2,4), (1,5), (3,2), (4,2), (3,1), (5,1)

(ii) $M = 6$; $N = 10$; (1,6), (2,1), (2,3), (3,5), (4,5), (4,2), (2,6), (5,3), (4,3), (6,4)

9.40. Suppose a graph G is input by means of an integer M, representing the vertices $1, 2, \ldots, M$, and a list of N ordered triples (a_i, b_i, w_i) of integers such that (a_i, b_i) is an edge of G and w_i is its weight. Write a procedure for each of the following:

(*a*) To find the $M \times M$ weight matrix W of the graph G.

(*b*) To use A and Warshall's algorithm to find the matrix Q of shortest paths between the vertices of G.

Test the above using the following data:

(i) $M = 4$; $N = 7$; (1,2,5), (2,4,2), (3,2,3), (1,1,7), (4,1,4), (4,3,1)

(ii) $M = 5$; $N = 8$; (3,5,3), (4,1,2), (5,2,2), (1,5,5), (1,3,1), (2,4,1), (3,4,4), (5,4,4)

LINKED REPRESENTATION OF GRAPHS

9.41. A weighted graph G with six vertices, $A, B, \ldots, F$, is stored in memory using a linked representation with a vertex file and an edge file as in Fig. 9-43.

(*a*) List the vertices in the order they appear in memory.

(*b*) Find the successor list succ (v) of each vertex v.

Vertex file

START 7

	1	2	3	4	5	6	7	8
VERTEX	*D*		*B*	*F*	*A*		*C*	*E*
NEXT-V	3		8	1	0		4	5
PTR	7		5	9	2		3	0

Edge file

	1	2	3	4	5	6	7	8	9	10	11	12
BEG-V	5	5	7		3	7	1		4	1	4	7
END-V	8	7	5		1	1	5		8	4	3	8
NEXT-E	0	1	12		0	0	10		11	0	0	6
WEIGHT	5	2	1		3	2	4		1	3	4	1

Fig. 9-43

9.42. Consider the weighted graph G whose linked representation appears in Fig. 9-43. Draw the graph of G.

9.43. Suppose a graph G is presented by the following table:

$$G = [A{:}B, C; \quad B{:}C, D; \quad C{:}C; \quad D{:}B; \quad E{:}\varnothing]$$

(*a*) Find the number of vertices and edges in G.

(*b*) Are there any sources or sinks?

(*c*) Draw the graph of G.

(*d*) Is G weakly connected? Unilaterally connected? Strongly connected?

9.44. Repeat Problem 9.43 for the table:

$$G = [A{:}D; \quad B{:}C; \quad C{:}E; \quad D{:}B, D, E; \quad E{:}A]$$

9.45. Repeat Problem 9.43 for the table:

$$G = [A{:}B, C, D, F; \quad B{:}E; \quad C{:}\varnothing; \quad D{:}\varnothing; \quad E{:}B, D, G; \quad F{:}D, G; \quad G{:}D]$$

9.46. Suppose Friendly Airways has eight daily flights serving the seven cities: Atlanta, Boston, Chicago, Denver, Houston, Philadelphia, Washington. Suppose the data on the flights are stored in memory as in Fig. 9-44; that is, using a linked representation where the cities and flights appear in linear sorted arrays. Draw a labeled directed graph G describing the data.

Vertex file

	1	2	3	4	5	6	7	8
CITY	*A*	*B*	*C*	*D*	*H*	*P*	*W*	
PTR	1	2	3	8	9	5	7	

Edge file

	1	2	3	4	5	6	7	8	9	10
NUMBER	101	102	201	202	203	301	302	401	402	
ORIG	1	2	3	1	6	6	7	4	5	
DEST	2	3	6	7	3	1	6	5	4	
NEXT-E	4	0	0	0	6	0	0	0	0	

Fig. 9-44

9.47. Using the data in Fig. 9-44, write a procedure with input CITYX and CITYY which finds the flight number of a direct flight from city X to city Y, if it exists. Test the procedure using:
(*a*) X = Atlanta, Y = Philadelphia; (*b*) X = Philadelphia, Y = Atlanta; (*c*) X = Houston, Y = Chicago; (*d*) X = Washington, Y = Chicago.

9.48. Using the data in Fig. 9-44, write a procedure with input CITYX and CITYY which finds the most direct route (minimum number of stops) from city X to city Y, if it exists. Test the procedure using the input in Problem 9.47.

MISCELLANEOUS PROBLEMS

9.49. Use the pruning algorithm to find the shortest path from s to t in Fig. 9-45.

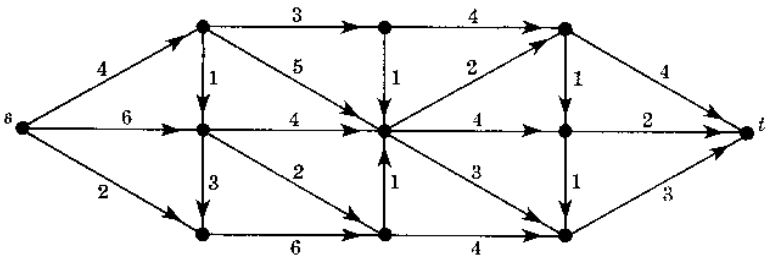


Fig. 9-45

9.50. Find a topological sort T of each of the following graphs:

(*a*) $G = [A{:}Z;\ B{:}T;\ C{:}B;\ D{:}\varnothing;\ X{:}D;\ Y{:}X;\ Z{:}B, X;\ S{:}C, Z;\ T{:}\varnothing]$

(*b*) $G = [A{:}X, Z;\ B{:}A;\ C{:}S, T;\ D{:}Y;\ X{:}S, T;\ Y{:}B;\ Z{:}\varnothing;\ S{:}Y;\ T{:}\varnothing]$

(*c*) $G = [A{:}C, S;\ B{:}T, Z;\ C{:}\varnothing;\ D{:}Z;\ X{:}A;\ Y{:}A;\ Z{:}X, Y;\ S{:}\varnothing;\ T{:}Y]$

Answers to Supplementary Problems

9.23. (*a*) Indegrees: 1, 1, 4, 3, 1; outdegrees: 2, 3, 1, 2, 2.
(*b*) None. (*c*) (v_1, v_2, v_4), (v_1, v_3, v_5, v_4), $(v_1, v_2, v_3, v_5, v_4)$.
(*d*) (v_3, v_5, v_4, v_3). (*e*) $(v_1, v_3), (v_1, v_2, v_3), (v_1, v_2, v_4, v_3), (v_1, v_2, v_1, v_3)$. (*f*) Unilaterally, but not strongly.

9.24. (*a*) Sources: v_1. (*b*) $(v_1, v_6, v_7, v_4), (v_1, v_6, v_7, v_2, v_2, v_5, v_3, v_4)$, (*c*) $(v_1, v_6, v_7, v_2, v_6, v_7, v_4)$.
(*d*) $(v_4, v_8, v_7, v_4), (v_4, v_8, v_7, v_2, v_5, v_3, v_4)$.

9.25. (*a*) succ (1) = [6], succ (3) = [4, 7], succ (5) = [3], succ (7) = [2, 4].
(*b*) (i) $(1, 6), (5, 3)$; (ii) $(2, 6), (6, 7), (7, 2), (3, 7)$.

9.26. (*a*) $G = [A{:}D;\ B{:}C;\ C{:}E;\ D{:}B, D, E;\ E{:}A]$. (*b*) Loop: (D, D).
(*c*) $(D, E), (D, B, C, E)$. (*d*) $(A, D, E, A), (A, D, B, C, E, A)$.
(*e*) Unilaterally, and strongly. (*f*) and (*g*) H has three edges: $(C, E), (D, E), (D, D)$. There are $8 = 2^3$ ways of choosing some of the three edges; and each choice gives a subgraph.

9.27. (*a*) $G = [A{:}B, C;\ B{:}E;\ C{:}D;\ D{:}A, E;\ E{:}\varnothing]$. (*b*) Sink: E. (*c*) $(A, B, E), (A, C, D, E)$.
(*d*) (A, C, D, A). (*e*) (C, D, A, B, E). (*f*) No.

9.28. See Fig. 9-46.

9.29. (*a*) See Fig. 9-47. (*b*) Only weakly.

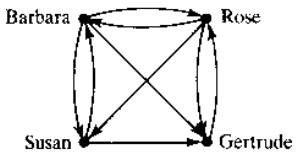


Fig. 9-46

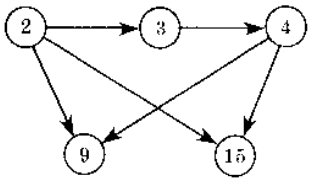


Fig. 9-47

9.30. *Hint*: Suppose $\alpha = (v_1, \ldots, v_m)$ is a longest path in G and does not include vertex u. If (u, v_1) is an arc, then $\beta = (u, \alpha)$ extends α. Hence (v_1, u) is an arc. If (u, v_2) is also an arc, then $\beta = (v_1, u, v_2, \ldots, v_m)$ extends α; hence (v_2, u) is an arc. Similarly $(v_3, u), \ldots, (v_m, u)$ are arcs. Hence $\beta = (\alpha, u)$ extends α. This contradicts the maximality of α.

9.31. (*a*) (i) (R, A, D), 2; (ii) (R, B, F, J), 3; (iii) (R, C, G), 2.
(*b*) H, E, I, J, G. (*c*) H:1.1.1, E:1.2, I:2.1.1, J:2.1.2, G:3.1,

9.32. (*a*) 0, 1, 1.1, 2, 2.1, 2.1.1, 2.2, 2.2.1, 2.2.1.1, 2.2.1.2, 3, 3.1, 3.1.1, 3.2.
(*b*) Fig. 9-48.

9.33. (*a*) Fig. 9-49. (*b*) $E = [/ \uparrow - * 3\ x * 5\ z\ 4 * a + *2\ b \uparrow c\ 2]$

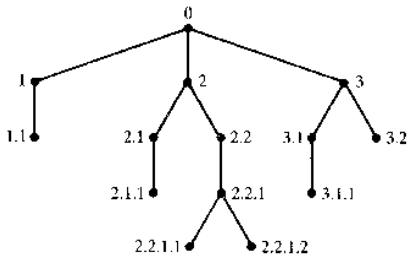


Fig. 9-48

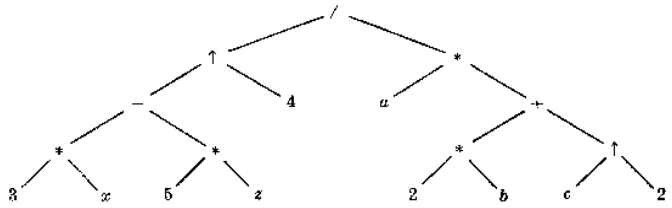


Fig. 9-49

9.34. (*a*) $A = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$; $P = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$.

(*b*) $0, 2, 1, 0, 0, \ldots$.
(*c*) Weakly and unilaterally.

9.35. (*a*) $A = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 2 & 0 & 0 \end{bmatrix}$; $P = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix}$.

(*b*) $0, 1, 1, 1, \ldots$.
(*c*) Weakly and unilaterally.

9.36. Let $P = [p_{ij}]$. For $i \neq j$, we have: (*a*) $p_{i,j} \neq 0$; (*b*) either $p_{i,j} \neq 0$ or $p_{j,i} \neq 0$.

9.37. (*a*) $A = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \end{bmatrix}$; $P = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \end{bmatrix}$

(*b*) (X, Z, Y, X).
(*c*) Unilaterally.

9.38. (*a*) $A = \begin{bmatrix} 0 & 7 & 0 & 0 \\ 3 & 0 & 2 & 0 \\ 0 & 0 & 0 & 5 \\ 6 & 1 & 4 & 0 \end{bmatrix}$; $Q = \begin{bmatrix} XYX & XY & XYS & XYST \\ YX & YSTY & YS & YST \\ STYX & STY & STYS & ST \\ TX & TY & TYS & TYST \end{bmatrix}$

9.39. (i) $A = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \end{bmatrix}$; $P = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 \end{bmatrix}$

(ii) $A = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}$; $P = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$

9.40. (i) $W = \begin{bmatrix} 7 & 5 & 0 & 0 \\ 0 & 0 & 0 & 2 \\ 0 & 3 & 0 & 0 \\ 4 & 0 & 1 & 0 \end{bmatrix}$; $Q = \begin{bmatrix} AA & AB & ABCD & ABD \\ BDA & BDCB & BDC & BD \\ CBDA & CB & CBDC & CBD \\ DA & DCB & DC & DCBD \end{bmatrix}$ where

A, B, C, D are the vertices.

(ii) $W = \begin{bmatrix} 0 & 0 & 1 & 0 & 5 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 4 & 3 \\ 2 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 4 & 0 \end{bmatrix}$; $Q = \begin{bmatrix} ACDA & ACEB & AC & ACD & ACE \\ BDA & BDACEB & BDAC & BD & BDACE \\ CDA & CEB & CDAC & CD & CE \\ DA & DACEB & DAC & DACD & DACEB \\ EDA & EB & EDAC & ED & EDACE \end{bmatrix}$

where A, B, C, D, E are the vertices.

9.41. (*a*) C, F, D, B, E, A; (*b*) [A:C, E; B:D; C:D, E, A; D:A, F; E:$\varnothing$; F:B, E].

9.42. See Fig. 9-50.

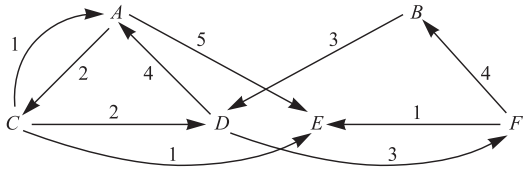


Fig. 9-50

9.43. (*a*) 5,6; (*b*) source, A; sink, C; (*c*) see Fig. 9-51(*a*); (*d*) none.

9.44. (*a*) 5,6; (*b*) none; (*c*) see Fig. 9-51(*b*); (*d*) all three.

9.45. (*a*) 7,11; (*b*) source, A; sinks, C, D; (*c*) see Fig. 9-51(*c*); (*d*) only weakly.

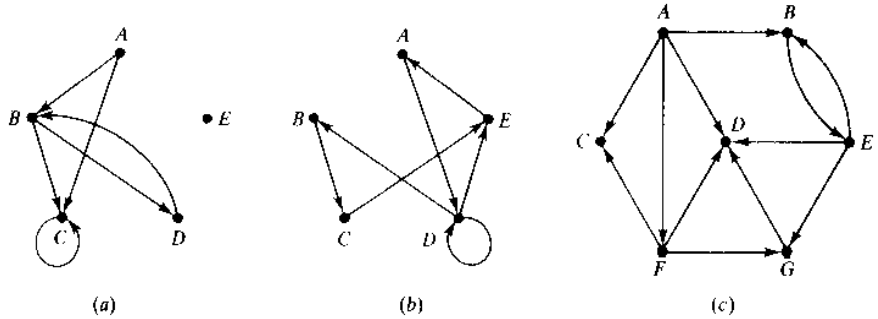


Fig. 9-51

9.46. See Fig. 9-52.

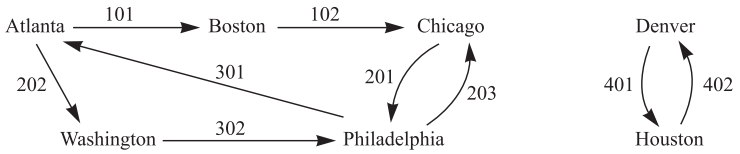


Fig. 9-52

9.47. (*a*) No; (*b*) yes; (*c*) no; (*d*) no.

9.48. (*a*) AWP; (*b*) PA; (*c*) none; (*d*) WPC.

9.49. $(s, 4, 1, 2, 1, 2, 1, 2, t)$.

9.50. *Hint*: First draw the graph. (*a*) $ASYCZBXTD$. (*b*) None, the graph is not cycle-free, e.g., (Y, B, A, X, S, Y) is a cycle. (*c*) $ZBTYXACSDZ$.

© The McGraw–Hill Companies, 2004

Chapter 10

Binary Trees

10.1 INTRODUCTION

The binary tree is a fundamental structure in mathematics and computer science. Some of the terminology of rooted trees, such as, edge, path, branch, leaf, depth, and level number, will also be used for binary trees. However, we will use the term node, rather than vertex, with binary trees. We emphasize that a binary tree is not a special case of a rooted tree; they are different mathematical objects.

10.2 BINARY TREES

A *binary tree* T is defined as a finite set of elements, called *nodes*, such that:

(1) T is empty (called the *null tree* or *empty tree*), or
(2) T contains a distinguished node R, called the *root* of T, and the remaining nodes of T form an ordered pair of disjoint binary trees T_1 and T_2.

If T does contain a root R, then the two trees T_1 and T_2 are called, respectively, the *left* and *right subtrees* of R. If T_1 is nonempty, then its root is called the *left successor* of R; similarly, it T_2 is nonempty, then its root is called the *right successor* of R.

The above definition of a binary tree T is recursive since T is defined in terms of the binary subtrees T_1 and T_2. This means, in particular, that every node N of T contains a left and a right subtree, and either subtree or both subtrees may be empty. Thus every node N in T has 0, 1, or 2 successors. A node with no successors is called a *terminal node*. Thus both subtrees of a terminal node are empty.

Picture of a Binary Tree

A binary tree T is frequently presented by a diagram in the plane called a *picture* of T. Specifically, the diagram in Fig. 10-1 represents a binary tree as follows:

(i) T consists of 11 nodes, represented by the letters A through L, excluding I.
(ii) The root of T is the node A at the top of the diagram.
(iii) A left-downward slanted line at a node N indicates a left successor of N; and a right-downward slanted line at N indicates a right successor of N.

Accordingly, in Fig. 10-1:

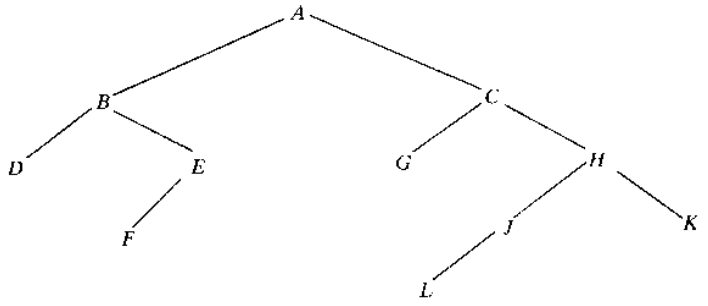


Fig. 10-1

(*a*) B is a left successor and C is a right successor of the root A.
(*b*) The left subtree of the root A consists of the nodes B, D, E, and F, and the right subtree of A consists of the nodes C, G, H, J, K, and L.
(*c*) The nodes A, B, C, and H have two successors, the nodes E and J have only one successor, and the nodes D, F, G, L, and K have no successors, i.e., they are terminal nodes.

Similar Binary Trees

Binary trees T and T' are said to be *similar* if they have the same structure or, in other words, if they have the same shape. The trees are said to be *copies* if they are similar and if they have the same contents at corresponding nodes.

EXAMPLE 10.1 Consider the four binary trees in Fig. 10-2. The three trees (*a*), (*c*), and (*d*) are similar. In particular the trees (*a*) and (*c*) are copies since they also have the same data at corresponding nodes. The tree (*b*) is neither similar nor a copy of the tree (*d*) because, in a binary tree, we distinguish between a left successor and a right successor even when there is only one successor.

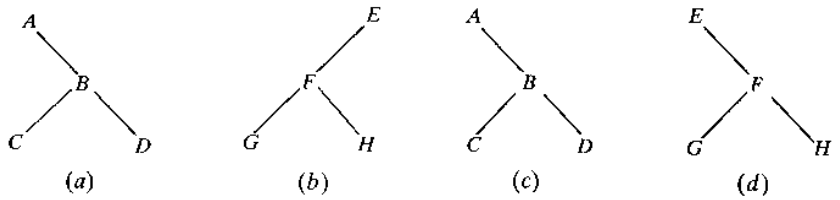


Fig. 10-2

Algebraic Expressions

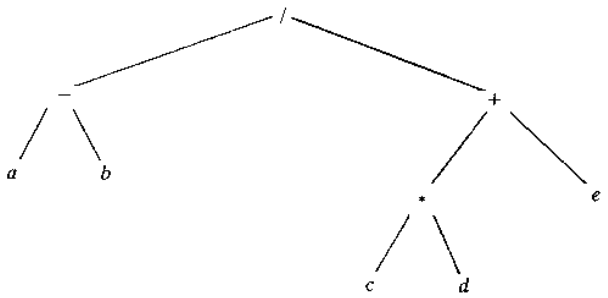
Consider any algebraic expression E involving only binary operations, such as

$$E = (a - b)/((c * d) + e)$$

E can be represented by means of the binary tree T pictured in Fig. 10-3. That is, each variable or constant in E appears as an "internal" node in T whose left and right subtrees correspond to the operands of the operation. For example:

(*a*) In the expression E, the operands of $+$ are $c * d$ and e.
(*b*) In the tree T, the subtrees of the node $+$ correspond to the subexpressions $c * d$ and e.

Clearly, every algebraic expression will correspond to a unique tree, and vice versa.



$$E = (a - b)/((c * d) + e).$$

Fig. 10-3

Terminology

Terminology describing family relationships is frequently used to describe relationships between the nodes of a tree T. Specifically, suppose N is a node in T with left successor S_1 and right successor S_2. Then N is called the *parent* (or *father*) of S_1 and S_2. Analogously, S_1 is called the *left child* (or *son*) of N, and S_2 is called the *right child* (or *son*) of N. Furthermore, S_1 and S_2 are said to be *siblings* (or *brothers*). Every node N in a binary tree T, except the root, has a unique parent, called the *predecessor* of N.

The terms descendant and ancestor have their usual meaning. That is, a node L is called a *descendant* of a node N (and N is called an *ancestor* of L) if there is a succession of children from N to L. In particular, L is called a *left* or *right descendant* of N according to whether L belongs to the left or right subtree of N.

Terminology from graph theory and horticulture is also used with a binary tree T. Specifically, the line drawn from a node N of T to a successor is called an *edge*, and a sequence of consecutive edges is called a *path*. A terminal node is called a *leaf*, and a path ending in a leaf is called a *branch*.

Each node in a binary tree T is assigned a *level number*, as follows. The root R of the tree T is assigned the level number 0, and every other node is assigned a level number which is 1 more than the level number of its parent. Furthermore, those nodes with the same level number are said to belong to the same *generation*.

The *depth* (or *height*) of a tree T is the maximum number of nodes in a branch of T. This turns out to be 1 more than the largest level number of T. The tree T in Fig. 10-1 has depth 5.

10.3 COMPLETE AND EXTENDED BINARY TREES

This section considers two special kinds of binary trees.

Complete Binary Trees

Consider any binary tree T. Each node of T can have at most two children. Accordingly, one can show that level r of T can have at most 2^r nodes. The tree T is said to be *complete* if all its levels, except possibly the last, have the maximum number of possible nodes, and if all the nodes at the last level appear as far left as possible. Thus there is a unique complete tree T_n with exactly n nodes (we are, of course, ignoring the contents of nodes). The complete tree T_{26} with 26 nodes appears in Fig. 10-4.

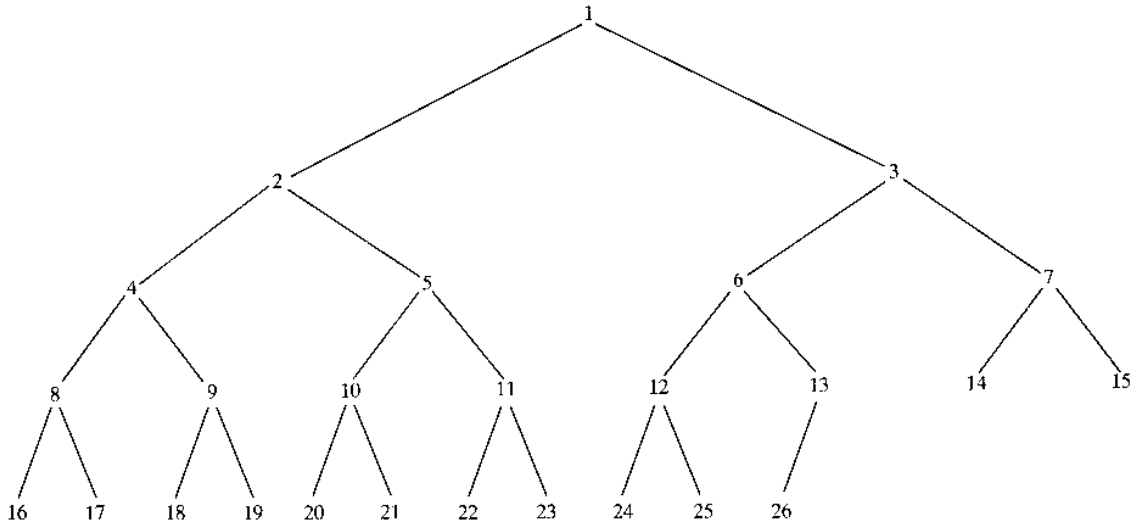


Fig. 10-4 Complete tree T_{26}.

The nodes of the complete binary tree T_{26} in Fig. 10-4 have been purposely labeled by the integers $1, 2, \ldots, 26$, from left to right, generation by generation. With this labeling, one can easily determine the children and parent of any node K in any complete tree T_n. Specifically, the left and right children of the node K are, respectively, $2 * K$ and $2 * K + 1$, and the parent of K is the node $[K/2]$. For example, the children of node 9 are the nodes 18 and 19, and its parent is the node $[9/2] = 4$. The depth d_n of the complete tree T_n with n nodes is given by

$$d_n = \lfloor \log_2 n + 1 \rfloor$$

This is a relatively small number. For example, if the complete tree T_n has $n = 1\,000\,000$ nodes, then its depth is $d_n = 21$.

Extended Binary Trees: 2-Trees

A binary tree tree T is said to be a *2-tree* or an *extended binary tree* if each node N has either 0 or 2 children. In such a case, the nodes with two children are called *internal nodes*, and the nodes with 0 children are called *external nodes*. Sometimes the nodes are distinguished in diagrams by using circles for internal nodes and squares for external nodes.

The term "extended binary tree" comes from the following operation. Consider any binary tree T, such as the tree in Fig. 10-5(*a*). Then T may be "converted" into a 2-tree by replacing each empty subtree by a new node, as pictured in Fig. 10-5(*b*). Observe that the new tree is, indeed, a 2-tree. Furthermore, the nodes in the original tree T are now the internal nodes in the extended tree, and the new nodes are the external nodes in the extended tree.

An important example of a 2-tree is the tree T corresponding to any algebraic expression E which uses only binary operations. As illustrated in Fig. 10-3, the variables in E will appear as the external nodes, and the operations in E will appear as internal nodes.

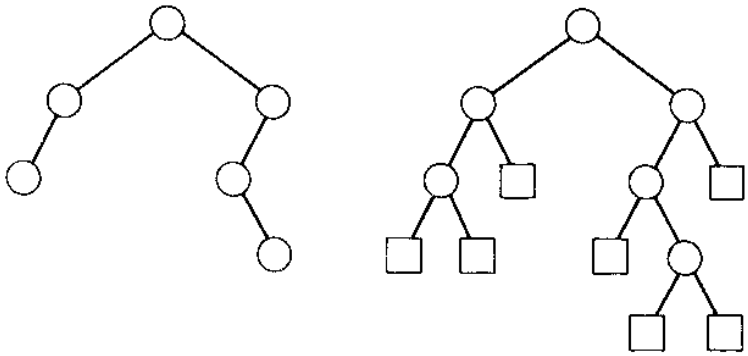


Fig. 10-5 Converting a binary tree T into a 2-tree.

10.4 REPRESENTING BINARY TREES IN MEMORY

Let T be a binary tree. This section discusses two ways of representing T in memory. The first and usual way is called the link representation of T and is analogous to the way linked lists are represented in memory. The second way, which uses a single array, called the sequential representation of T. The main requirement of any representation of T is that one should have direct access to the root R of T and, given any node N of T, one should have direct access to the children of N.

Linked Representation of Binary Trees

Consider a binary tree T. Unless otherwise stated or implied, T will be maintained in memory by means of a *linked representation* which uses three parallel arrays, INFO, LEFT, and RIGHT, and a pointer variable ROOT as follows. First of all, each node N of T will correspond to a location K such that:

(1) INFO[K] contains the data at the node N.
(2) LEFT[K] contains the location of the left child of node N.
(3) RIGHT[K] contains the location of the right child of node N.

Furthermore, ROOT will contain the location of the root R of T. If any subtree is empty, then the corresponding pointer will contain the null value; if the tree T itself is empty, then ROOT will contain the null value.

Remark 1: Most of our examples will show a single item of information at each node N of a binary tree T. In actual practice, an entire record may be stored at the node N. In other words, INFO may actually be a linear array of records or a collection of parallel arrays.

Remark 2: Any invalid address may be chosen for the null pointer denoted by NULL. In actual practice, 0 or a negative number is used for NULL.

EXAMPLE 10.2 Consider the binary tree T in Fig. 10-1. A schematic diagram of the linked representation of T appears in Fig. 10-6. Observe that each node is pictured with three fields, and the empty subtrees are pictured by using $\times$ for the null entries. Figure 10-7 shows how this linked representation of T may appear in memory, where we

have written linear arrays vertical rather than horizontal for notational convenience. Note that ROOT = 5 points to INFO[5] = *A* since *A* is the root of *T*. Also, note that LEFT[5] = 10 points to INFO[10] = *B* since *B* is the left child of *A*, and RIGHT[5] = 2 points to INFO[2] = *C* since *C* is the right child of *A*. The choice of 18 elements for the arrays is arbitrary.

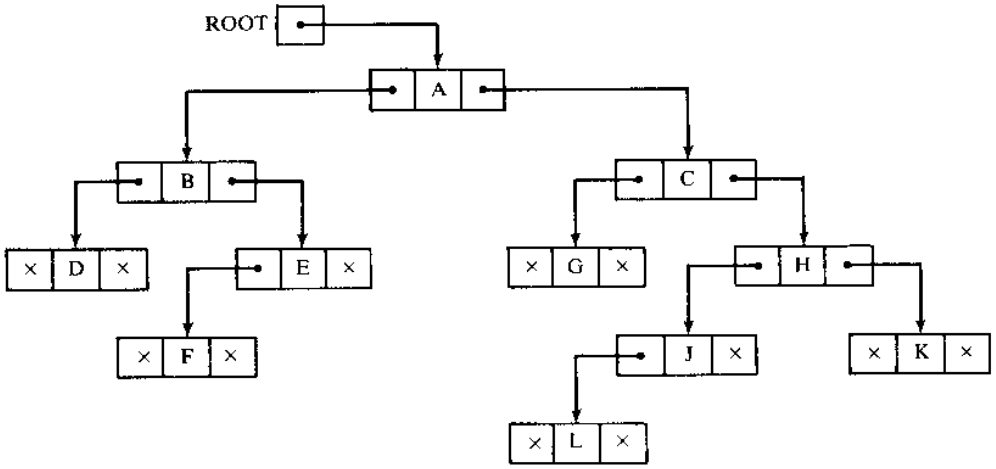


Fig. 10-6

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
INFO	*K*	*C*	*G*		*A*	*H*	*L*			*B*		*F*	*E*			*J*	*D*	
LEFT	0	3	0		10	16	0			17		0	12			7	0	
RIGHT	0	6	0		2	1	0			13		0	0			0	0	

ROOT 5

Fig. 10-7

Sequential Representation of Binary Trees

Suppose *T* is a binary tree that is complete or nearly complete. Then there is an efficient way of maintaining *T* in memory called the *sequential representation* of *T*. This representation uses only a single linear array TREE together with a pointer variable END as follows:

(*a*) The root *R* of *T* is stored in TREE[1].
(*b*) If a node *N* occupies TREE[*K*], then its left child is stored in TREE[$2 * K$] and its right child is stored in TREE[$2 * K + 1$].
(*c*) END contains the location of the last node of *T*.

Furthermore, the node *N* at TREE[*K*] contains an empty left or right subtree according as $2 * K$ or $2 * K + 1$ exceeds END or according as TREE[$2 * K$] or TREE[$2 * K + 1$] contains the NULL value.

The sequential representation of the binary tree *T* in Fig. 10-8(*a*) appears in Fig. 10-8(*b*). Observe that we require 14 locations in the array TREE even though *T* has only 9 nodes. Generally speaking, the sequential representation of a tree with depth *d* will require an array with approximately 2^d elements. Accordingly, this sequential representation is usually inefficient unless, as stated above, the binary tree *T* is complete or nearly complete. For example, the tree *T* in Fig. 10-1 has 11 nodes and depth 5, which means it would require an array with approximately $2^5 = 32$ elements.

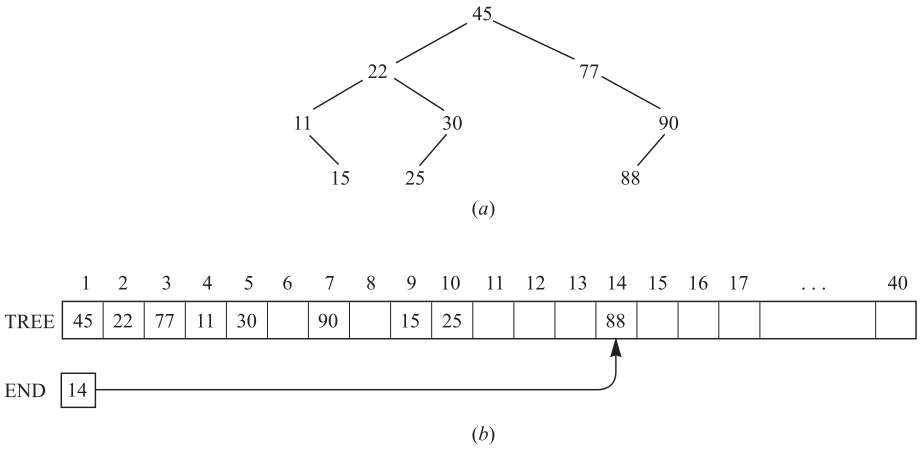


Fig. 10-8

10.5 TRAVERSING BINARY TREES

There are three standard ways of traversing a binary tree T with root R. These three algorithms, called *preorder*, *inorder*, and *postorder*, are as follows:

Preorder:
(1) Process the root R.
(2) Traverse the left subtree of R in preorder.
(3) Traverse the right subtree of R in preorder.

Inorder:
(1) Traverse the left subtree of R in inorder.
(2) Process the root R.
(3) Traverse the right subtree of R in inorder.

Postorder:
(1) Traverse the left subtree of R in postorder.
(2) Traverse the right subtree of R in postorder.
(3) Process the root R.

Observe that each algorithm contains the same three steps, and that the left subtree of R is always traversed before the right subtree. The difference between the algorithms is the time at which the root R is processed. Specifically, in the "pre" algorithm, the root R is processed before the subtrees are traversed; in the "in" algorithm, the root R is processed between the traversals of the subtrees; and in the "post" algorithm, the root R is processed after the subtrees are traversed.

The three algorithms are sometimes called, respectively, the node-left-right (NLR) traversal, the left-node-right (LNR) traversal and the left-right-node (LRN) traversal.

EXAMPLE 10.3 Consider the binary tree in Fig. 10-9. Observe that A is the root, that its left subtree L_T consists of nodes B, D, and E, and its right subtree R_T consists of nodes C and F.

(*a*) The preorder traversal of T processes A, traverses L_T, and traverses R_T. However, the preorder traversal of L_T processes the root B and then D, and E, and the preorder traversal of R_T processes the root C and then F. Hence $ABDECF$ is the preorder traversal of T.

(*b*) The inorder traversal of T traverses L_T, processes A, and traverses R_T. However, the inorder traversal of L_T processes D, B, and then E, and the inorder traversal of R_T processes C and then F. Hence $DBEACF$ is the inorder traversal of T.

(*c*) The postorder traversal of T traverses L_T, traverses R_T, and processes A. However, the postorder traversal of L_T processes D, E, and then B, and the postorder traversal of R_T processes F and then C. Accordingly, $DEBFCA$ is the postorder traversal of T.

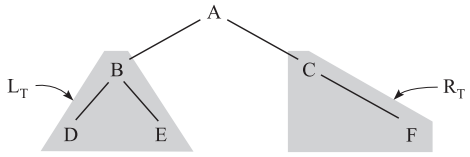


Fig. 10-9

EXAMPLE 10.4 Consider the binary tree T in Fig. 10-10. The preorder traversal is as follows:

(Preorder) A B D E F C G H J L K

This order is the same as the one obtained by scanning the tree from the left as indicated by the path in Fig. 10-10. That is, one "travels" down the leftmost branch until meeting a terminal node, then one backtracks to the next branch, and so on. In the preorder traversal, the rightmost terminal node, node K, is the last node scanned. Observe that the left subtree of the root A is traversed before the right subtree, and both are traversed after A. The same is true for any other node having subtrees, which is the underlying property of a preorder traversal.

The reader can verify by inspection that the other two ways of traversing the tree T in Fig. 10-10 are as follows:

(Inorder) D B F E A G C L J H K
(Postorder) D F E B G L J K H C A

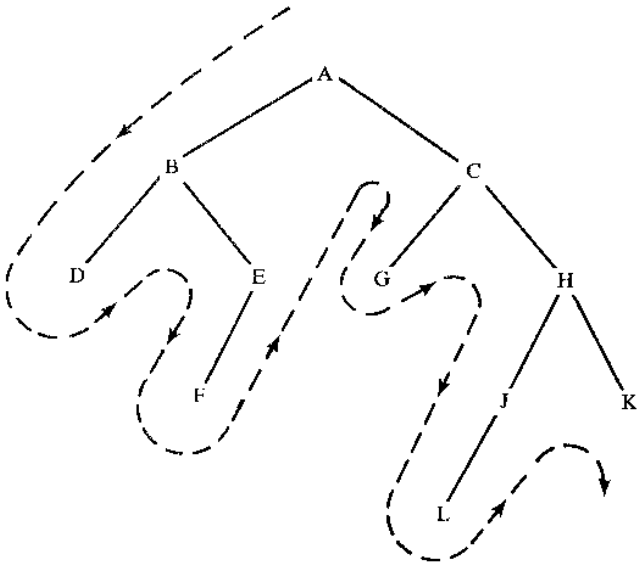


Fig. 10-10

Remark: Observe that the terminal nodes, D, F, G, L, and K, of the binary tree in Fig. 10-10 are traversed in the same order, from left to right, in all three traversals. We emphasize that this is true for any binary tree T.

10.6 BINARY SEARCH TREES

This section discusses one of the most important data structures in computer science, a binary search tree. This structure enables us to search for and find an element with an average running time $f(n) = O(\log_2 n)$, where n is the number of data items. It also enables us to easily insert and delete elements. This structure contrasts with the following structures:

(*a*) *Sorted linear array*: Here one can search for and find an element with running time $f(n) = O(\log_2 n)$. However, inserting and deleting elements is expensive since, on the average, it involves moving $O(n)$ elements.
(*b*) *Linked list*: Here one can easily insert and delete elements. However, it is expensive to search and find an element, since one must use a linear search with running time $f(n) = O(n)$.

Although each node in a binary search tree may contain an entire record of data, the definition of the tree depends on a given field whose values are distinct and may be ordered.

Definition: Suppose T is a binary tree. Then T is called a *binary search tree* if each node N of T has the following property:

> The value of N is greater than every value in the left subtree of N and is less than every value in the right subtree of N.

It is not difficult to see that the above property guarantees that the inorder traversal of T will yield a sorted listing of the elements of T.

Remark: The above definition of a binary search tree assumes that all the node values are distinct. There is an analogous definition of a binary search tree T which admits duplicates, that is, in which each node N has the following properties:

(*a*) $N > M$ for every node M in a left subtree of N.
(*b*) $N \leq M$ for every node M in a right subtree of N.

When this definition is used, the operations discussed below must be modified accordingly.

EXAMPLE 10.5 The binary tree T in Fig. 10-11(*a*) is a binary search tree. That is, every node N in T exceeds every number in its left subtree and is less than every number in its right subtree. Suppose the 23 were replaced by 35. Then T would still be a binary search tree. On the other hand, suppose the 23 were replaced by 40. Then T would not be a binary search tree, since 40 would be in the left subtree of 38 but $40 > 38$.

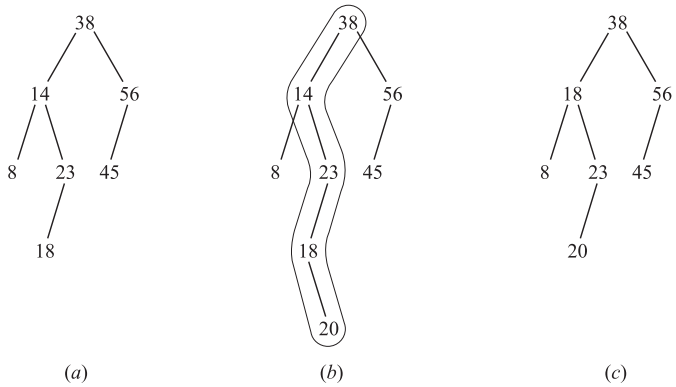


Fig. 10-11

(*a*) ***Searching and Inserting in a Binary Search Tree***: The following is a search and insertion algorithm in a binary search tree T.

Algorithm 10.6A: A binary search tree T and an ITEM of information is given. The algorithm finds the location of ITEM in T, or inserts ITEM as a new node in the tree.

Step 1. Compare ITEM with the root N of the tree.
(*a*) If ITEM $< N$, proceed to the left child of N.
(*b*) If ITEM $> N$, proceed to the right child of N.

Step 2. Repeat Step 1 until one of the following occurs:
(*a*) We meet a node N such that ITEM $= N$. In this case the search is successful.
(*b*) We meet an empty subtree, which indicates the search is unsuccessful. Insert ITEM in place of the empty subtree.

Step 3. Exit.

EXAMPLE 10.6 Consider the binary search tree T in Fig. 10-11(*a*). Suppose ITEM $= 20$ is given, and we want to find or insert ITEM into T. Simulating Algorithm 10-6A, we obtain the following steps:

(1) Compare ITEM $= 20$ with root $R = 38$. Since $20 < 38$, proceed to the left child of 38, which is 14.
(2) Compare ITEM $= 20$ with 14. Since $20 > 14$, proceed to the right child of 14, which is 23.
(3) Compare ITEM $= 20$ with 23. Since $20 < 23$, proceed to the left child of 23, which is 18.
(4) Compare ITEM $= 20$ with 18. Since $20 > 18$ and 18 has no right child, insert 20 as the right child of 18.

Figure 10-11(*b*) shows the new tree with ITEM $= 20$ inserted. The path down the tree during the algorithm has been ringed.

(*b*) ***Deleting in a Binary Search Tree***: The following is an algorithm which deletes a given ITEM from a binary search tree T. It uses Algorithm 10.6A to find the location of ITEM in T.

Algorithm 10.6B: A binary search tree T and an ITEM of information is given. $P(N)$ denotes the parent of a node N, and $S(N)$ denotes the inorder successor of N. The algorithm deletes ITEM from T.

Step 1. Use Algorithm 10.6A to find the location of the node N which contains ITEM and keep track of the location of the parent node $P(N)$. (If ITEM is not in T, then STOP and Exit.)

Step 2. Determine the number of children of N. There are three cases:
- (a) N has no children. N is deleted from T by simply replacing the location of N in the parent node $P(N)$ by the NULL pointer.
- (b) N has exactly one child M. N is deleted from T by replacing the location of N in the parent node $P(N)$ by the location of M. (This replaces N by M.)
- (c) N has two children.
  - (i) Find the inorder successor $S(N)$ of N. (Then $S(N)$ has no left child.)
  - (ii) Delete $S(N)$ from T using (a) or (b).
  - (iii) Replace N by $S(N)$ in T.

Step 3. Exit.

Remark: Observe that case (iii) in Step 2(c) is more complicated than the first two cases. The inorder successor $S(N)$ of N is found as follows. From the node N, move right to the right child of N, and then successively move left until meeting a node M with no left child. The node M is the inorder successor $S(N)$ of N.

EXAMPLE 10.7 Consider the binary tree T in Fig. 10-11(b). Suppose we want to delete ITEM $= 14$ from T. First find the node N such that $N = 14$. Note $N = 14$ has two children. Moving right and then left, we find the inorder successor $S(N) = 18$ of N. We delete $S(N) = 18$ by replacing it by its only child 20, then we replace $N = 14$ by $S(N) = 18$. This yields the tree in Fig. 10-11(c).

Complexity of the Binary Search Tree Algorithms

Let T be a binary tree with n nodes and depth d, and let $f(n)$ denote the running time of either of the above algorithms. Algorithm 10.6A tells us to proceed from the root R down through the tree T until finding ITEM in T or inserting ITEM as a terminal node. Algorithm 10.6B tells us to proceed from the root R down through the tree T to find ITEM and then to continue down the tree T to find the inorder successor of ITEM. In either case, the number of moves cannot exceed the depth d of the tree. Thus the running time $f(n)$ of either algorithm depends on the depth d of the tree T.

Now suppose T has the property that, for any node N of T, the depths of the subtrees of N differ by at most 1. Then the tree T is said to be *balanced*, and $d \sim \log_2 n$. Therefore, the running time $f(n)$ of either algorithm in a balanced tree is very fast; specifically, $f(n) = O(\log_2 n)$. On the other hand, as items are added into a binary search tree T, there is no guarantee that T remains balanced. It could even happen that $d \sim n$. In this case, $f(n)$ would be relatively slow; specifically, $f(n) = O(n)$. Fortunately, there are techniques for rebalancing a binary search tree T as elements are added to T. Such techniques, however, lie beyond the scope of this text.

10.7 PRIORITY QUEUES, HEAPS

Let S be a priority queue. That is, S is a set where elements may be periodically inserted and deleted, but where the current largest element (element with highest priority) is always deleted. One may maintain S in memory as follows:

(*a*) ***Linear array***: Here one can easily insert an element by simply adding it to the end of the array. However, it is expensive to search for and find the largest element, since one must use a linear search with running time $f(n) = O(n)$.

(*b*) ***Sorted linear array***: Here the largest element is either first or last, and so it is easily deleted. However, inserting and deleting elements is expensive since, on the average, it involves moving $O(n)$ elements.

This section introduces a discrete structure which can efficiently implement a priority queue S.

Heaps

Suppose H is a complete binary tree with n elements. We assume H is maintained in memory using its sequential representation, not a linked representation. (See Section 10.4.)

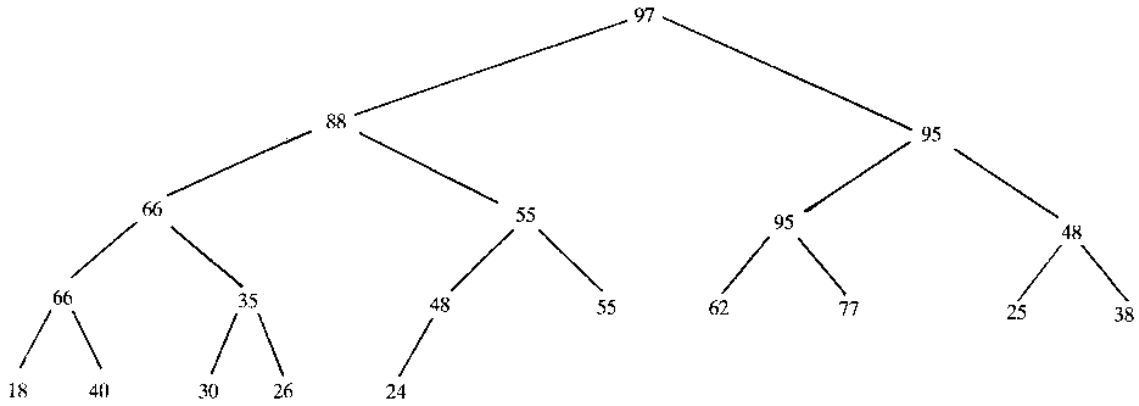
Definition: Suppose H is a complete binary tree. Then H is called a *heap*, or a *maxheap*, if each node N has the following property.

> The value of N is greater than or equal to the value at each of the children of N.

Accordingly, in a heap, the value of N exceeds the value of every one of its decendents. In particular, the root of H is a largest value of H.

A *minheap* is defined analogously: The value of N is less than or equal to the value at each of its children.

EXAMPLE 10.8 Consider the complete binary tree H in Fig. 10-12(*a*). Observe that H is a heap. This means, in particular, that the largest element of H appear at the "top" of the heap. Fig. 10-12(*b*) shows the sequential representation of H by the array TREE and the variable END. Accordingly:



(*a*) Heap.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	. . .	30
TREE	97	88	95	66	55	95	48	66	35	48	55	62	77	25	38	18	40	30	26	24		. . .	

END 20

(*b*) Sequential representation.

Fig. 10-12

(*a*) TREE[1] is the root R of H.

(*b*) TREE[$2K$] and TREE[$2K + 1$] are the left and right children of TREE[K].

(*c*) The variable END = 20 points to the last element in H.

(*d*) The parent of any nonroot node TREE(J) is the node TREE[$J \div 2$] (where $J \div 2$ means integer division).

Observe that the nodes of H on the same level appear one after another in the array TREE. The choice of 30 locations for TREE is arbitrary.

(*a*) ***Inserting into a Heap***: The following algorithm inserts a given ITEM of information into a heap H.

Algorithm 10.7: *A* heap H and a new ITEM are given. The algorithm inserts ITEM into H.

Step 1. Adjoin ITEM at the end of H so that H is still a complete tree, but not necessarily a heap.

Step 2. (Reheap) Let ITEM rise to its "appropriate place" in H so that H is a heap. That is:
(*a*) Compare ITEM with its parent P(ITEM). If ITEM $>$ P(ITEM), then interchange ITEM and P(ITEM).
(*b*) Repeat (*a*) until ITEM $\leq$ P(ITEM).

Step 3. Exit.

Remark: One must verify that the above algorithm does always yield a heap as a final tree. This is not difficult to see, and we leave this verification to the reader.

EXAMPLE 10.9 Consider the heap H in Fig. 10-12. Suppose we want to insert ITEM = 70 into H. Simulating Algorithm 10.7A, we first adjoin ITEM as the last element of the complete tree; that is, we set TREE[21] = 70 and END = 21. Then we reheap, i.e., we let ITEM rise to its appropriate place as follows:

(*a*) Compare ITEM = 70 with its parent 48. Since $70 > 48$, we interchange 70 and 48.

(*b*) Compare ITEM = 70 with its new parent 55. Since $70 > 55$, we interchange 70 and 55.

(*c*) Compare ITEM = 70 with its parent 88. Since $70 < 88$, ITEM = 70 has risen to its appropriate place in H.

Figure 10-13 shows the final tree H with ITEM = 70 inserted. The path up the tree by ITEM has been circled.

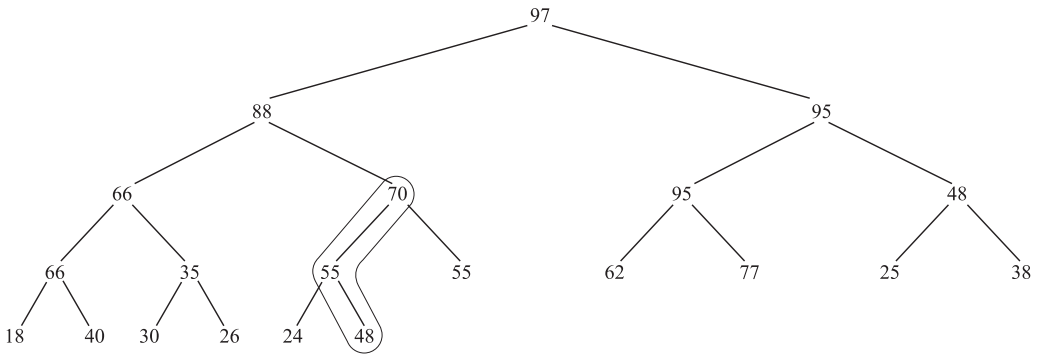


Fig. 10-13 ITEM = 70 is inserted.

(*b*) ***Deleting the Root from a Heap***: The following algorithm deletes the root R from a heap H.

Algorithm 10-7B: The algorithm deletes the root R from a given heap H.

Step 1. Assign the root R to some variable ITEM.

Step 2. Replace the deleted root R by the last node of L of H so that H is still a complete binary tree, but not necessarily a heap. [That is, set TREE[1] := TREE[END] and then set END := END−1.]

Step 3. (Reheap) Let L sink to its "appropriate place" in H so that H is a heap. That is:
(*a*) Find the larger child LARGE(L) of L. If $L <$ LARGE(L), then interchange L and LARGE(L).
(*b*) Repeat (*a*) until $L \geq$ LARGE(L).

Step 4. Exit.

Remark: As with inserting in a heap, one must verify that the above algorithm does always yield a heap as a final tree. Again, we leave this verification to the reader. We also note that Step 3 may not end until the node L reaches the bottom of the tree, i.e., until L has no children.

EXAMPLE 10.10 Consider the heap H in Fig. 10-14(*a*), where $R = 95$ is the root and $L = 22$ is the last node of H. Suppose we want to delete $R = 95$ from the heap H. Simulating Algorithm 10.7B, we first assign ITEM = 95, and then we replace $R = 95$ by $L = 22$. This yields the complete tree in Fig. 10-14(*b*), which is not a heap. (Note that both subtrees of 22 are still heaps.) Then we reheap, i.e., we let $L = 22$ sink to its appropriate place as follows:

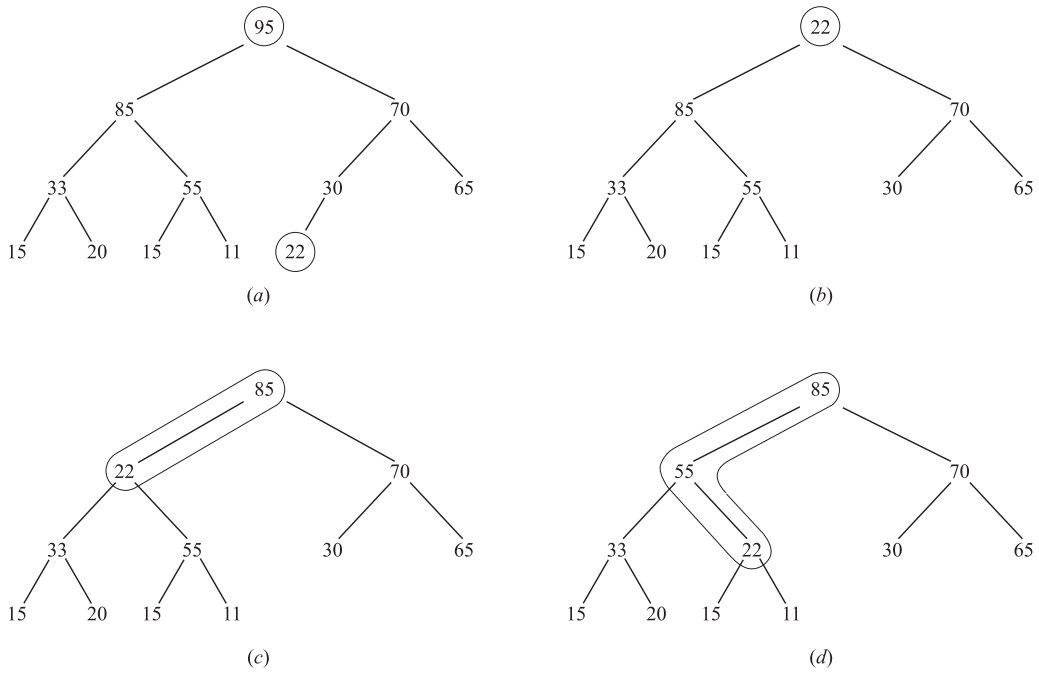


Fig. 10-14

(*a*) The children of $L = 22$ are 85 and 70. The larger is 85. Since $22 < 85$, interchange 22 and 85. This yields the tree in Fig. 10-14(*c*).

(*b*) The children of $L = 22$ are now 33 and 55. The larger is 55. Since $22 < 55$, interchange 22 and 55. This yields the tree in Fig. 10.14(*d*).

(*c*) The children of $L = 22$ are now 15 and 11. The larger is 15. Since $22 \geq 15$, the node $L = 22$ has sunk to its appropriate place in the heap.

Thus Fig. 10-14(*d*) is the required heap H without its original root $R = 95$. Observe that we ringed the paths as $L = 22$ made its way down the tree.

Complexity of the Heap Algorithms

Let H be a heap with n nodes. Since H is a complete tree, $d \approx \log_2 n$ where d is the depth of H. Algorithm 10.7A tells us to let the new ITEM proceed up the tree, from level to level, until finding its appropriate place in H. Algorithm 10.7B tells us to let the original last node L proceed down the tree, level by level, until finding its appropriate place in H. In either case, the number of moves cannot exceed the depth d of H. Thus the running time $f(n)$ of either algorithm is very fast; specifically, $f(n) = O(\log_2 n)$. Accordingly, the heap is a much more efficient way to implement a priority queue S than either the linear array or sorted linear array mentioned at the beginning of the section.

10.8 PATH LENGTHS, HUFFMAN'S ALGORITHM

Let T be an extended binary tree or 2-tree (Section 10.3). That is, T is a binary tree where each node N has either 0 or 2 children. The nodes with no children are called *external nodes*, and the nodes with two children are called *internal nodes*. Sometimes the nodes are distinguished in diagrams by using circles for internal nodes and squares for external nodes. Moreover, if T has n external nodes, then T has $n - 1$ internal nodes. Figure 10-15 shows a 2-tree with seven external nodes and hence $7 - 1 = 6$ internal nodes.

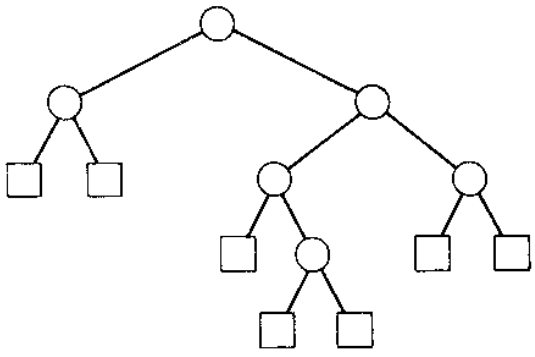


Fig. 10-15

Weighted Path Lengths

Suppose T is a 2-tree with n external nodes, and suppose each external node is assigned a (non-negative) weight. The *weighted path length* (or simply *path length*) P of the tree T is defined to be the sum

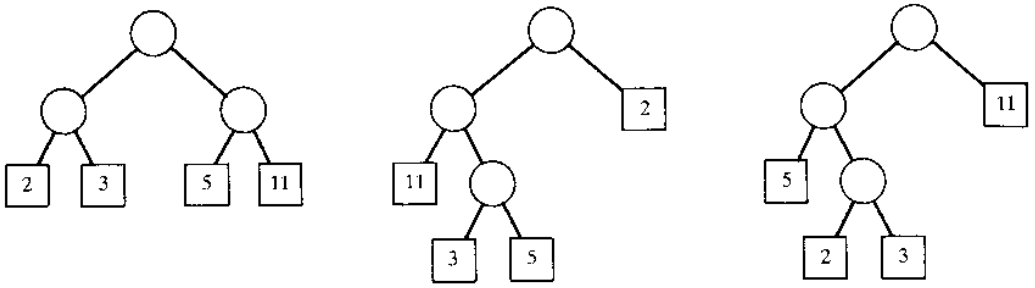
$$P = W_1L_1 + W_2L_2 + \cdots + W_nL_n$$

where W_i is the weight at an external node N_i and L_i is the length of the path from the root R to the node N_i. (The path length P exists even for nonweighted 2-trees where one simply assumes the weight 1 at each external node.)

EXAMPLE 10.11 Figure 10-16 shows three 2-trees, T_1, T_2, and T_3, each having external nodes with the same weights 2, 3, 5, and 11. The weighted path lengths of the three trees are as follows:

$$P_1 = 2(2) + 3(2) + 5(2) + 11(2) = 42$$
$$P_2 = 2(1) + 3(3) + 5(3) + 11(2) = 48$$
$$P_3 = 2(3) + 3(3) + 5(2) + 11(1) = 36$$

The quantities P_1 and P_3 indicate that the complete tree need not give a minimum path length P, and the quantities P_2 and P_3 indicate that similar trees need not give the same path lengths.



(*a*) T_1. (*b*) T_2. (*c*) T_3.

Fig. 10-16

Huffman's Algorithm

The general problem we want to solve is the following. Suppose a list of n weights is given, say,

$$w_1, w_2, \ldots, w_n$$

Among all the 2-trees with n external nodes and with the given n weights, find a tree T with a minimum weighted path length. (Such a tree T is seldom unique.) Huffman gave an algorithm to find such a tree T.

Huffman's algorithm, which follows, is recursively defined in terms of the number n of weights. In practice, we use an equivalent iterated form of the Huffman algorithm which constructs the desired tree T from the bottom up rather than from the top down.

Algorithm 10.8 (Huffman): The algorithm recursively finds a weighted 2-tree T with n given weights $w_1, w_2, \ldots, w_n$ which has a minimum weighted path length.

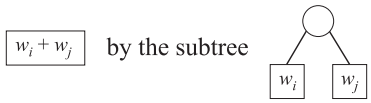
Step 1. Suppose $n = 1$. Let T be the tree with one node N with weight w_1, and then Exit.

Step 2. Suppose $n > 1$.

(*a*) Find two minimum weights, say w_i and w_j, among the n given weights.

(*b*) Find a tree T' which gives a minimum weighted path length for the $n - 1$ weights

(*c*) In the tree T', replace the external node



(*d*) Exit.

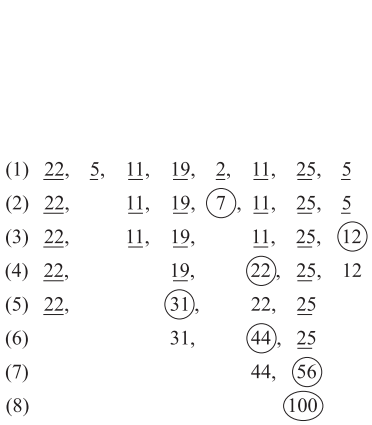
EXAMPLE 10.12 Let A, B, C, D, E, F, G, H be eight data items with the following assigned weights:

Data item:	A	B	C	D	E	F	G	H
Weight:	22	5	11	19	2	11	25	5

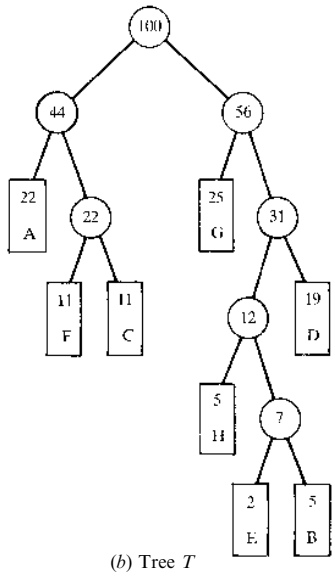
Construct a 2-tree T with a minimum weighted path length P using the above data as external nodes.

Apply the Huffman algorithm. That is, repeatedly combine the two subtrees with minimum weights into a single subtree as shown in Fig. 10-17(*a*). For clarity, the original weights are underlined, and a circled number indicates the root of a new subtree. The tree T is drawn from Step (8) backward yielding Fig. 10-17(*b*). (When splitting a node into two parts, we have drawn the smaller node on the left.) The path length P follows:

$$P = 22(2) + 11(3) + 11(3) + 25(2) + 5(4) + 2(5) + 5(5) + 19(3) = 280$$



(*a*) Huffman algorithm



(*b*) Tree T

Fig. 10-17

Computer Implementation of Huffman's Algorithm

Consider again the data in Example 10.12. Suppose we want to implement the algorithm using the computer. Since some of the nodes in our binary tree are weighted, our tree can be maintained by four parallel arrays: INFO, WT, LEFT, and RIGHT. The first eight columns in Fig. 10-18 shows how the data may be stored in the computer initially.

Each step in Huffman's algorithm assigns values to WT, LEFT, and RIGHT in columns 9 through 15, which correspond, respectively, to steps (2) through (8) in Fig. 10-17. Specifically, each step finds the current two minimal weights and their locations, and then enters the sum in WT and their locations in LEFT and RIGHT. For example, the current minimal weights after assigning values to column 11, which corresponds to step (*d*), are 12 and 19 appearing in WT[10] and WT[4]. Accordingly, we assign WT[12] = 12 + 19 = 31 and LEFT[12] = 10 and RIGHT[12] = 4. The last step tells us that ROOT = 15, or we use that fact that ROOT = $2n - 1$, where $n = 8$ is the number of external nodes. Thus all of Fig. 10-18 gives the required tree T.

	1	2	3	4	5	6	7	8		9	10	11	12	13	14	15	16
INFO	*A*	*B*	*C*	*D*	*E*	*F*	*G*	*H*									
WT	22	5	11	19	2	11	25	5		7	12	22	31	44	56	100	
LEFT	0	0	0	0	0	0	0	0		5	8	6	10	1	7	13	
RIGHT	0	0	0	0	0	0	0	0		2	9	3	4	11	12	14	
										(2)	(3)	(4)	(5)	(6)	(7)	(8)	

ROOT 15

Fig. 10-18

Remark: During the execution of Huffman's algorithm we need to keep track of the current weights and to find two of the minimal weights. This may be efficiently accomplished by maintaining an auxiliary minheap, where each node contains a weight and its location in the tree. We use a minheap rather than a maxheap since we want the node with the lowest weight to be on the top of the heap.

Application to Coding

Suppose a collection of n data items $A_1, A_2, \ldots, A_n$, are to be coded by means of strings of bits. One way to do this is to code each item by an r-bit string where

$$n < 2^r$$

For example, a 48-character set may be coded in memory using 6-bit strings. One cannot use 5-bit strings since $2^5 = 32 < 48$.

Suppose the data items do not occur with the same probability. Then memory space and time may be conserved by using variable-length strings, where items which occur frequently are assigned shorter strings and items which occur infrequently are assigned longer strings. For example, country telephone codes use this principle. The country code for United States is simply 1, for France is 33, and for Finland is 358. This section discusses a coding using variable length that is based on the *Huffman tree* T for weighted data items, that is, a 2-tree T with minimum path length P.

Huffman Code: Suppose n data items $A_1, A_2 \ldots, A_n$ are assigned weights, and suppose T is a Huffman tree for the data. Each edge in T is assigned 0 or 1 according as the edge points to a left child or to a right child. The Huffman code assigns to each external node A_i the sequence of bits from the root R of the tree T to the node A_i.

The above Huffman code has the "prefix" property, that is, the code of any item is not an initial substring of the code of any other item. This means that there cannot be any ambiguity in decoding any message using a Huffman code.

EXAMPLE 10.13 Consider again the eight data items A, B, C, D, E, F, G, H in Example 10-12. Suppose the weights represent the percentage probabilities that the items will occur. Assigning bit labels to the edges in the Huffman tree in Fig. 10-17(*b*), we obtain the tree T in Fig. 10-19. The reader can verify that the tree T yields the following code:

A: 00	*B*: 11011,	*C*: 011,	*D*: 111
E: 11010,	*F*: 010	*G*: 10,	*H*: 1100

This is an efficient coding of the data items.

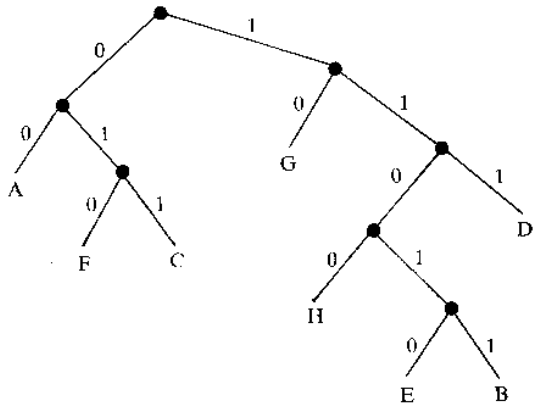


Fig. 10-19

10.9 GENERAL (ORDERED ROOTED) TREES REVISITED

Let T be an ordered rooted tree (Section 9.4), which is also called a *general tree*. T may be formally defined as a nonempty set of elements, called *nodes*, such that:

(1) T contains a distinguished element R, called the *root* of T.
(2) The remaining elements of T form an ordered collection of zero or more disjoint trees $T_1, T_2, \ldots, T_m$.

The trees $T_1, T_2, \ldots, T_m$ are called *subtrees* of the root R, and the roots of $T_1, T_2, \ldots, T_m$ are called *successors* of R.

Terminology from family relationships, graph theory, and horticulture is used for general trees in the same way as for binary trees. In particular, if N is a node with successors $S_1, S_2, \ldots, S_m$, then N is called the *parent* of the S_i, the S_i are called *children* of N, and the S_i are called *siblings* of each other.

EXAMPLE 10.14 Figure 10-20 is a picture of a general tree T with 13 nodes,

$$A, B, C, D, E, F, G, H, J, K, L, M, N$$

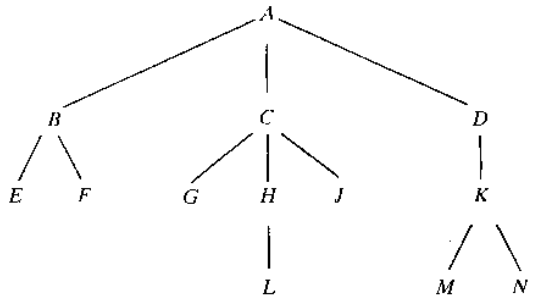


Fig. 10-20

Unless otherwise stated, the root of a tree T is the node at the top of the diagram, and the children of a node are ordered from left to right. Accordingly, A is the root of T, and A has three children; the first child B, the second child C and the third child D. Observe that:

(*a*) The node C has three children.

(*b*) Each of the nodes B and K has two children.

(*c*) Each of the nodes D and H has only one child.

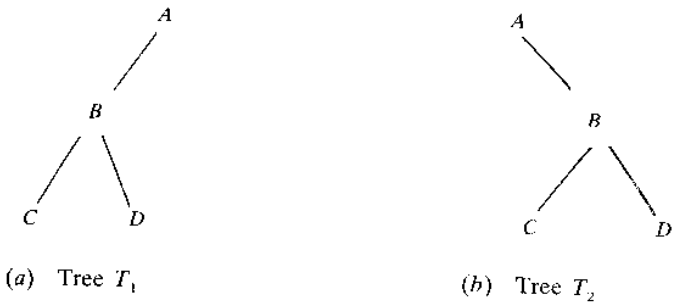
(*d*) The nodes, E, F, G, L, J, M and N have no children.

The last group of nodes, those with no children, are called *terminal nodes*.

Remark: A binary tree T' is not a special case of a general tree T. They are two different objects. The two basic differences follow:

(1) A binary tree T' may be empty, but a general tree T is nonempty.
(2) Suppose a node N has only one child. Then the child is distinguished as a left child or right child in a binary tree T', but no such distinction exists in a general tree T.

The second difference is illustrated by the trees T_1 and T_2 in Fig. 10-21. Specifically, as binary trees, T_1 and T_2 are distinct trees, since B is the left child of A in the tree T_1 but B is the right child of A in the tree T_2. On the other hand, there is no difference between the trees T_1 and T_2 as general trees.



(*a*) Tree T_1 (*b*) Tree T_2

Fig. 10-21

Forest

A *forest* F is defined to be an ordered collection of zero or more distinct trees. Clearly, if we delete the root R from a general tree T, then we obtain the forest F consisting of the subtrees of R (which may be empty). Conversely, if F is a forest, then we may adjoin a node R to F to form a general tree T where R is the root of T and the subtrees of R consist of the original trees in F.

Computer Representation of General Trees

Suppose T is a general tree. Unless otherwise stated or implied, T will be maintained in memory by means of a linked representation which uses three parallel arrays INFO, CHILD (or DOWN), and SIBL (or HORZ), and a pointer variable ROOT as follows. First of all, each node N of T will correspond to a location K such that:

(1) INFO[K] contains the data at node N.
(2) CHILD[K] contains the location of the first child of N. The condition CHILD[K] = NULL indicates that N has no children.
(3) SIBL[K] contains the location of the next sibling of N. The condition SIBL[K] = NULL indicates that N is the last child of its parent.

Furthermore, ROOT will contain the location of the root R of T. Although this representation may seem artificial, it has the important advantage that each node N of T, regardless of the number of children of N, will contain exactly three fields.

The above representation may easily be extended to represent a forest F consisting of trees $T_1, T_2, \ldots, T_m$ by assuming the roots of the trees are siblings. In such a case, ROOT will contain the location of the root R_1 of the first tree T_1; or when F is empty, ROOT will equal NULL.

EXAMPLE 10.15 Consider the general tree T in Fig. 10-20. Suppose the data of the nodes of T are stored in an array INFO as in Fig. 10-22(*a*). The structural relationships of T are obtained by assigning values to the pointer ROOT and the arrays CHILD and SIBL as follows:

(*a*) Since the root A of T is stored in INFO[2], set ROOT:= 2.

(*b*) Since the first child of A is the node B, which is stored in INFO[3], set CHILD[2]:= 3. Since A has no sibling, set SIBL[2]: = NULL.

(*c*) Since the first child B is the node E, which is stored in INFO[15], set CHILD[3]: = 15. Since node C is the next sibling of B and C is stored in INFO[4], set SIBL[3]: = 4.

And so on. Figure 10-22(*b*) gives the final values in CHILD and SIBL.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
INFO		*A*	*B*	*C*		*G*	*H*	*J*	*N*	*M*	*L*	*K*		*F*	*E*	*D*

(*a*)

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
CHILD		3	15	6		0	11	0	0	0	0	10		0	0	12
SIBL		0	4	16		7	8	0	0	9	0	0		0	14	0

ROOT 2

(*b*)

Fig. 10-22

Correspondence between General Trees and Binary Trees

Suppose T is a general tree. Then we may assign a unique binary tree T' to T as follows. First of all, the nodes of the binary tree T' will be the same as the nodes of the general tree T, and the root of T' will be the root of T. Let N be an arbitrary node of the binary tree T'. Then the left child of N in T' will be the first child of the node N in the general tree T and the right child of N in T' will be the next sibling of N in the general tree T.

The computer representation of the general tree T and the linked representation of the corresponding binary tree T' are exactly the same except that the names of the arrays CHILD and SIBL for the general tree T will correspond to the names of the arrays LEFT and RIGHT for the binary tree T'. The importance of this correspondence is that certain algorithms that applied to binary trees, such as the traversal algorithms, may now apply to general trees.

EXAMPLE 10.16 Consider the general tree T in Fig. 10-20. The reader can verify that the binary tree T' in Fig. 10-23 corresponds to the general tree T. Observe that by rotating counterclockwise the picture of T' in Fig. 10-23 until the edges pointing to the right children are horizontal, we obtain a picture in which the nodes occupy the same relative position as the nodes in Fig. 10-20. Furthermore, a computer representation of the binary tree T' can be obtained by simply changing CHILD to LEFT and SIBL to RIGHT in the computer representation of the general tree T in Fig. 10-22.

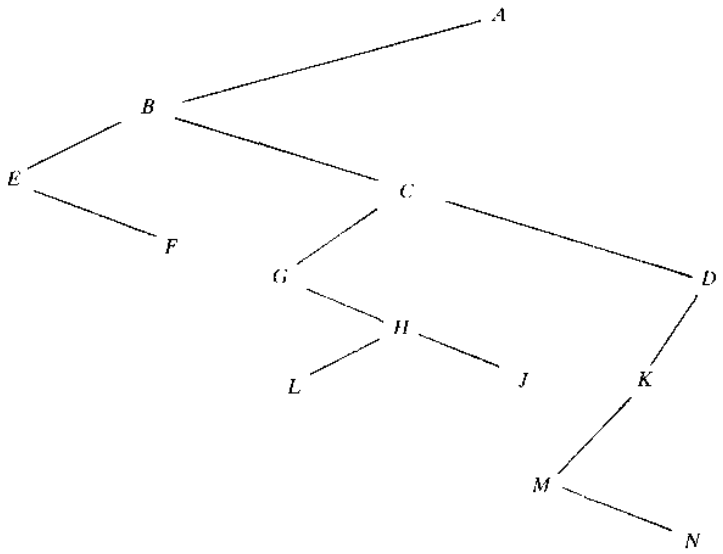


Fig. 10-23 Binary tree T'.

Solved Problems

BINARY TREES

10.1. Suppose T is the binary tree stored in memory as in Fig. 10-24. Draw the diagram of T.

The tree T is drawn from its root R downward as follows:

(*a*) The root R is obtained from the value of the pointer ROOT. Note that ROOT = 5. Hence INFO[5] = 60 is the root R of T.

(*b*) The left child of R is obtained from the left pointer field of R. Note that LEFT[5] = 2. Hence INFO[2] = 30 is the left child of R.

(*c*) The right child of R is obtained from the right pointer field of R. Note that RIGHT[5] = 6. Hence INFO[6] = 70 is the right child of R.

We can now draw the top part of the tree as pictured in Fig. 10-25(*a*). Repeating the above process with each new node, we finally obtain the required tree T in Fig. 10-25(*b*).

	1	2	3	4	5	6	7	8	9	10	11	12	13	14
INFO	20	30	40	50	60	70	80	90			35	45	55	95
LEFT	0	1	0	0	2	0	0	7			0	3	11	0
RIGHT	0	13	0	0	6	8	0	14			12	4	0	0

ROOT 5

Fig. 10-24

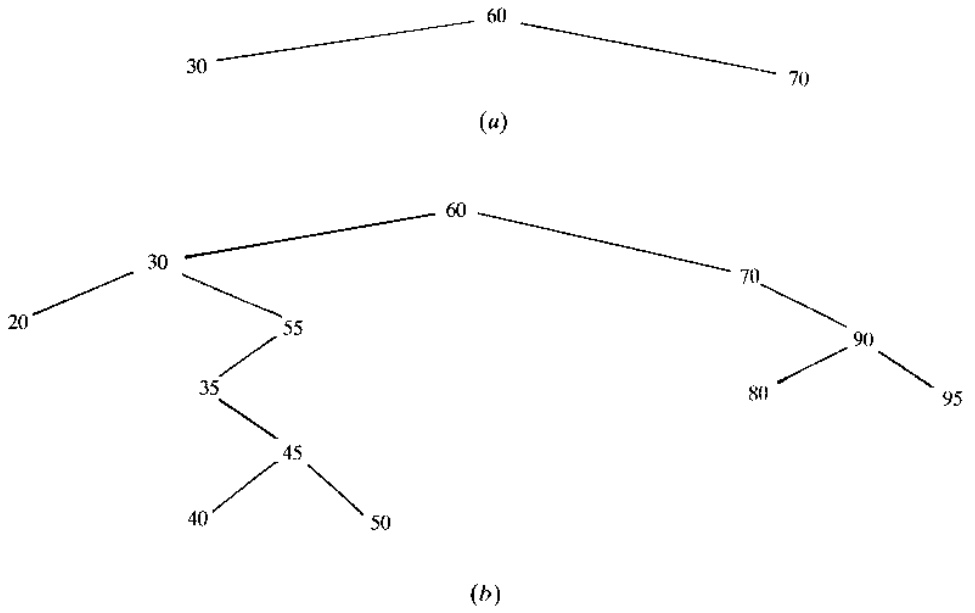


Fig. 10-25

10.2. Consider the three trees T_1, T_2, T_3 in Fig. 10-26. Identify those which represent the same: (*a*) rooted tree, (*b*) ordered rooted tree, (*c*) binary tree.

(*a*) They all represent the same rooted tree, that is, A is the root with children (immediate successors) B and C and C has the single child D.

(*b*) Here T_1 and T_2 are the same ordered rooted tree but T_3 is different. Specifically, B is the first child of A in T_1 and T_2 but the second child of A in T_3.

(*c*) They all represent different binary trees. Specifically, T_1 and T_2 are different since we distinguish between left and right successors even when there is only one successor (which is not true for ordered rooted trees). That is, D is a left successor of C in T_1 but a right successor of C in T_2.

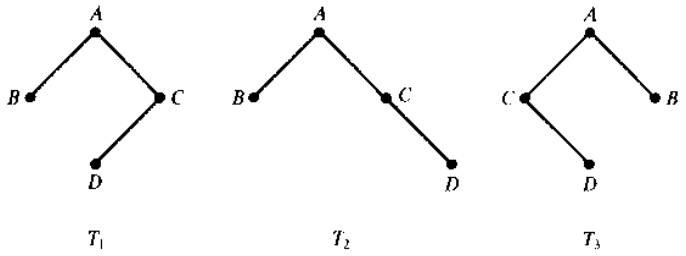


Fig. 10-26

10.3. Consider the binary tree T in Fig. 10-27. Find the sequential representation of T in memory.

The sequential representation of T uses only a single linear array TREE together with a variable pointer END.

(*a*) The root R of T is stored in TREE[1]; hence TREE[1] = F.

(*b*) If node N occupies TREE[K], then its left and right children are stored in TREE[$2 * K$] and TREE[$2 * K + 1$], respectively. Thus TREE[2] = A and TREE[3] = D since A and D are the left and right children of F. And so on. Figure 10-28 contains the sequential representation of T. Note that TREE[10] = C since C is the left child of K, which is stored in TREE[5]. Also, TREE[14] = B and TREE[15] = E since B and E are the left and right children of G, which is stored in TREE[7].

(*c*) END points to the location of the last node of T; hence END = 15.

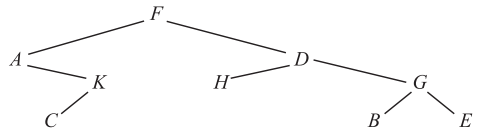


Fig. 10-27

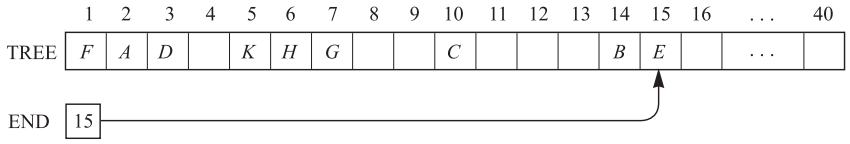


Fig. 10-28

10.4. Consider the binary tree T in Fig. 10-27.

(*a*) Find the depth d of T, and how is d related to the sequential representation of T.

(*b*) Traverse T using the preorder algorithm.

(*c*) Traverse T using the inorder algorithm.

(*d*) Traverse T using the postorder algorithm.

(*e*) Find the terminal nodes of T, and the order that they are traversed in (*b*), (*c*), and (*d*).

(*a*) The depth d is the number of nodes in a longest branch of T; hence $d = 4$. (We note that END always lies between 2^d and 2^{d+1}; specifically, $s^2 \leq \text{END} < 2^{d+1}$. As expected, $8 \leq \text{END} < 16$.)

(*b*) The preorder traversal of T is a recursive NLR algorithm, that is, it first processes a node N, then its left subtree L, and finally its right subtree R. Letting $[A_1, \ldots, A_k]$ denote a subtree with nodes $A_1, \ldots, A_k$, and the tree T is traversed as follows:

$$F\text{–}[A, K, C][D, H, G, B, E] \qquad \text{or} \qquad F\text{–}A\text{–}[K, C]\text{–}D\text{–}[H][G, B, E]$$

or, finally,

$$F\text{–}A\text{–}K\text{–}C\text{–}D\text{–}H\text{–}G\text{–}B\text{–}E$$

(*c*) The inorder traversal of T is a recursive LNR algorithm, that is, first processes a left subtree L, then its node N, and finally its right subtree R. Thus T is traversed as follows:

$$[A, K, C]\text{–}F\text{–}[D, H, G, B, E] \qquad \text{or} \qquad A\text{–}[K, C]\text{–}F\text{–}[H]\text{–}D\text{–}[G, B, E]$$

or finally,

$$A\text{–}K\text{–}C\text{–}F\text{–}H\text{–}D\text{–}G\text{–}B\text{–}E$$

(*d*) The postorder traversal of T is a recursive LRN algorithm, that is, it first processes a left subtree L, then its right subtree R, and finally its node N. Thus T is traversed as follows:

$$[A, K, C][D, H, G, B, E]\text{–}F \qquad \text{or} \qquad [K, C]\text{–}A\text{–}[H][G, B, E]\text{–}D\text{–}F$$

or, finally,

$$C–K–A–H–B–E–G–D–A$$

(*e*) The terminal nodes are the nodes without children. They are traversed in the same order in all three traversal algorithms: C, H, B, E.

10.5. A binary tree T has nine nodes. Draw the diagram of T if the preorder and inorder traversals of T yield the following sequences of nodes:

Preorder:	G	B	Q	A	C	P	D	E	R
Inorder:	Q	B	C	A	G	P	E	D	R

The tree T is drawn from its root R downward as follows.

(*a*) The root of T is obtained by choosing the first node in its preorder. Thus G is the root of T.

(*b*) The left child of node G is obtained as follows. First use the inorder of T to find the nodes in the left subtree T_1 of G. Thus T_1 consists of the nodes Q, B, C, A, which are to the left of G in the inorder of T. Then the left child of G is obtained by choosing the first node (root) in the preorder of T_1 which appears in the preorder of T. Thus B is the left child of G.

(*c*) Similarly, the right subtree T_2 of G consists of the nodes P, E, D, R; and P is the root of T_2, that is, P is the right child of G.

Repeating the above process with each new node, we finally obtain the required tree T in Fig. 10-29.

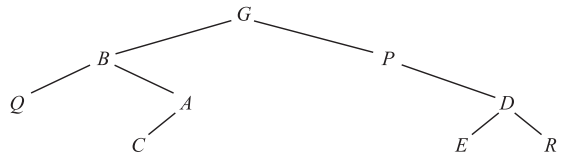


Fig. 10-29

10.6. Consider the algebraic expression $E = (2x + y)(5a - b)^3$.

(*a*) Draw the tree T which corresponds to the expression E.

(*b*) Find the *scope* of the exponential operator; that is, find the subtree rooted at the exponential operator.

(*c*) Find the preorder of T.

(*a*) Use an arrow ($\uparrow$) for exponentiation and an asterisk ($*$) for multiplication to obtain the tree shown in Fig. 10-30.

(*b*) The scope of $\uparrow$ is the subtree shaded in Fig. 10-30. It corresponds to the subexpression $(5a - b)^3$.

(*c*) Scan the tree from the left (as in Fig. 10-10) to obtain

$$* + *2\,x\,y \uparrow - *\,5\,a\,b\,3$$

(This is precisely the prefix Polish notation for the algebraic expression E.)

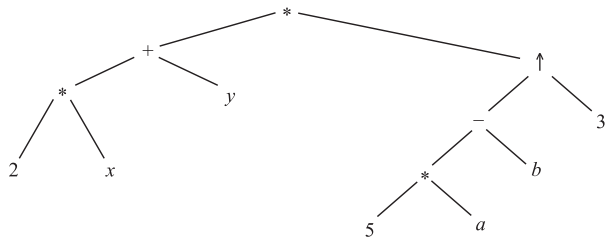


Fig. 10-30

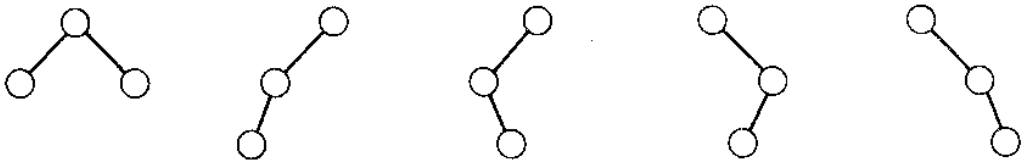
10.7. Draw all possible nonsimilar trees T where:

(*a*) T is a binary tree with three nodes.

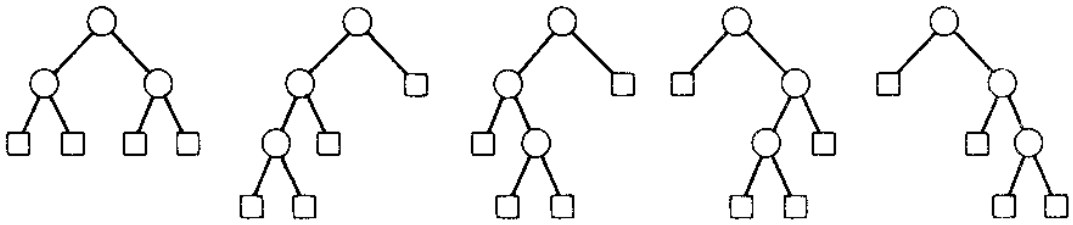
(*b*) T is a 2-tree with four external nodes.

(*a*) There are five such trees, which are pictured in Fig. 10-31(*a*).

(*b*) Each 2-tree with four external nodes is determined by a binary tree with three nodes, that is, by a tree in part (*a*). Thus there are five such trees which are pictured in Fig. 10-31(*b*).



(*a*) Binary trees with 3 nodes.



(*b*) Extended binary trees with 4 external nodes.

Fig. 10-31

BINARY SEARCH TREES, HEAPS

10.8. Consider the binary tree T in Fig. 10-25(*b*).

(*a*) Why is T a binary search tree?

(*b*) Suppose ITEM = 33 is added to the tree. Find the new tree T.

(*a*) T is a binary search tree since each node N is greater than the values in its left subtree and less than the values in its right subtree.

(*b*) Compare ITEM = 3 with the root, 60. Since $33 < 60$, move to the left child, 30. Since $33 > 60$, move to the right child, 55. Since $33 < 55$, move to the left child, 35. Now $33 < 35$, but 35 has no left child.

Hence add ITEM = 33 as a left child of the node 35 to give the tree in Fig. 10-32. The shaded edges indicate the path down through the tree during the insertion.

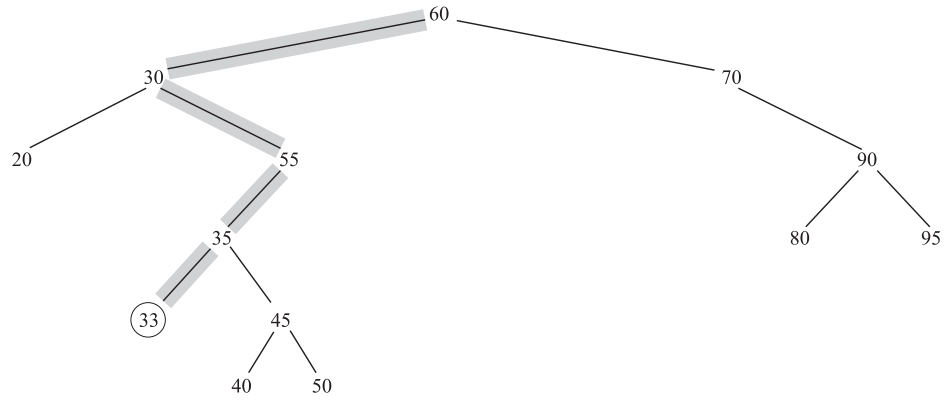


Fig. 10-32

10.9. Suppose the following list of letters is inserted into an empty binary search tree:

$$J, \quad R, \quad D, \quad G, \quad W, \quad E, \quad M, \quad H, \quad P, \quad A, \quad F, \quad Q$$

(*a*) Find the final tree T. (*b*) Find the inorder traversal of T.

(*a*) Insert the nodes one after the other to obtain the tree T in Fig. 10-33.

(*b*) The inorder traversal of T follows:

$$A, \quad D, \quad E, \quad F, \quad G, \quad H, \quad J, \quad M, \quad P, \quad Q, \quad R, \quad W$$

Observe that this is the alphabetical listing of the letters. [The inorder traversal of any binary search tree T yields a sorted list of the nodes.]

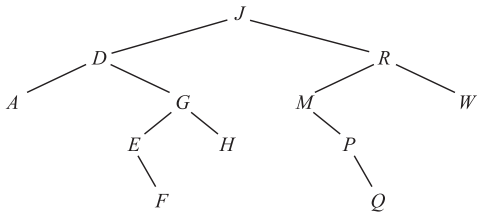


Fig. 10-33

10.10. Consider the binary search tree T in Fig. 10-33. Describe the tree T after (*a*) the node M is deleted, and (*b*) the node D is deleted.

(*a*) The node M has only one child, P. Hence delete M and let P become the left child of R in place of M.

(*b*) The node D has two children. Find the inorder successor of D, which is the node E. First delete E from the tree, and then replace D by the node E.

Figure 10-34 shows the updated tree T.

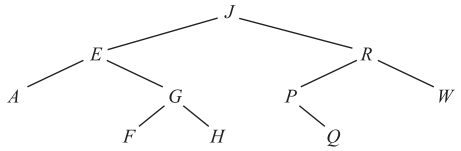


Fig. 10-34

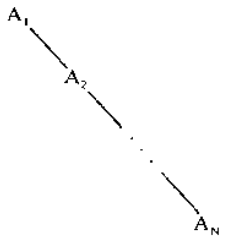


Fig. 10-35

10.11. Suppose n data items $A_1, A_2, \ldots, A_N$ are already sorted, i.e., $A_1 < A_2 < \cdots < A_N$.

(*a*) If the items are inserted in order into an empty binary tree T, describe the final tree T.

(*b*) What is the depth d of the final tree T.

(*c*) Compare d with the average depth d^* of a binary tree with n nodes for (i) $n = 50$; (ii) $n = 100$; (iii) $n = 500$.

(*a*) The tree T will consist of one branch which extends to the right as pictured in Fig. 10-35.

(*b*) The branch of T has n nodes; hence $d = n$.

(*c*) It is known that $d^* = c \log_2 n$, where $c \approx 1.4$. Hence:

(i) $d(50) = 50$; $d^*(50) \approx 9$.

(i) $d(100) = 100$; $d^*(100) \approx 10$.

(i) $d(500) = 500$; $d^*(500) \approx 12$.

10.12. Consider the minheap H in Fig. 10-36(*a*). (H is a *minheap*, since the smaller elements are on top of the heap, rather than the larger elements.) Describe the heap after ITEM = 11 is inserted into H.

First insert ITEM as the next node in the complete tree, that is, as the left child of node 44. Then repeatedly compare ITEM with its PARENT, and interchange ITEM and PARENT as long as ITEM < PARENT. Since $11 < 44$, interchange 11 and 44. Since $11 < 22$, interchange 11 and 22. Since $11 > 8$, ITEM = 11 has found its appropriate place in the heap H. Figure 10-36(*b*) shows the final heap H. The shaded edges indicate the path of ITEM up the tree.

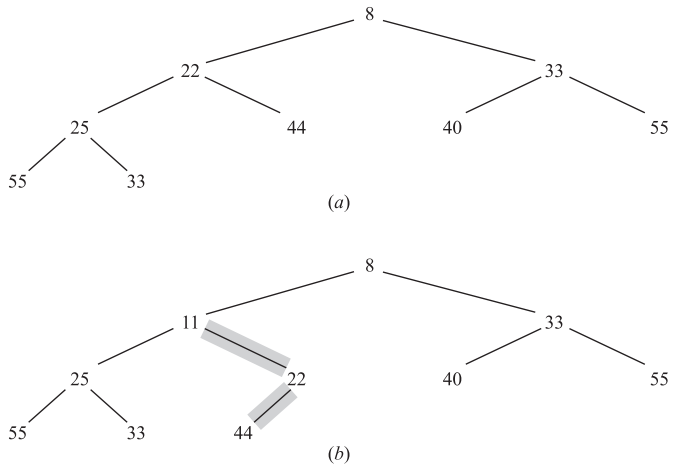


Fig. 10-36

10.13. Consider the complete tree T with $N = 6$ nodes in Fig. 10-37, and assume T is stored sequentially in an array A. Form a heap H out of T by repeatedly inserting $A[J + 1]$ into the heap $A[1]$ to $A[J]$ (as in Problem 10.12) for $J = 1, 2, \ldots, N - 1$.

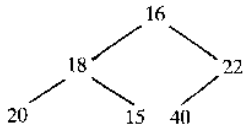


Fig. 10-37

Figure 10-38 shows the different steps. We explain each step separately.

(*a*) $J = 1$ and ITEM $= A[2] = 18$. Since $18 > 16$, interchange 18 and 16.

(*b*) $J = 2$ and ITEM $= A[3] = 22$. Since $22 > 18$, interchange 22 and 18.

(*c*) $J = 3$ and ITEM $= A[4] = 20$. Since $20 > 16$ but $20 < 22$, interchange only 20 and 16.

(*d*) $J = 4$ and ITEM $= A[5] = 15$. Since $15 < 20$, no interchanges take place.

(*e*) $J = 5$ and ITEM $= A[6] = 40$. Since $40 > 18$ and $40 > 22$, first interchange 40 and 18 and then interchange 40 and 22.

The tree is now a heap. The dotted edges indicate that an exchange has taken place. The unshaded area indicates that part of the tree which forms a heap. Observe that the heap is created from the top down (although individual elements move up the tree).

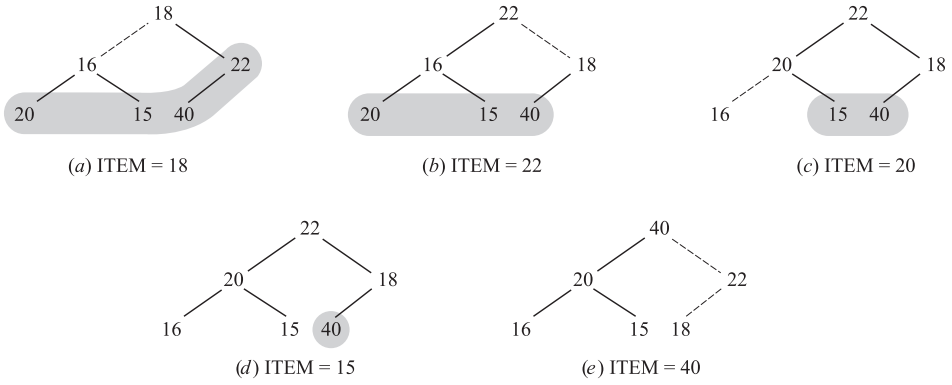


Fig. 10-38

PATH LENGTHS, HUFFMAN'S ALGORITHM

10.14. Consider the weighted 2-tree T in Fig. 10-39. Find the weighted path length P of the tree T.

Multiply each weight W_i by the length L_i of the path from the root of T to the node containing the weight, and then sum all such products to obtain P. Thus:

$$P = 4(2) + 15(4) + 25(4) + 5(3) + 8(2) + 16(2)$$
$$= 8 + 60 + 100 + 15 + 16 + 32 = 231$$

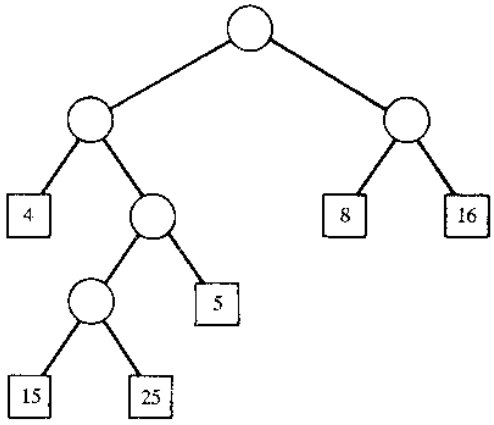


Fig. 10-39

10.15. Suppose the six weights 4, 15, 25, 5, 8, 16 are given. Find a 2-tree with the given weights and a minimum path length P. (Compare T with the tree in Fig. 10-39.)

Use the Huffman algorithm. That is, repeatedly combine the two subtrees with minimum weights into a single subtree as follows:

(*a*) 4, 15, 25, 5, 8, 16 (*d*) 25, 17, 31*

(*b*) 15, 25, 9,* 8, 16 (*e*) 42,* 31

(*c*) 15, 25, 17,* 16 (*f*) 73*

(The circled number indicates the root of the new subtree in the step.) The tree T is drawn from Step (*f*) backward, yielding Fig. 10-40. With the tree T compute:

$$P = 25(2) + 4(4) + 5(4) + 8(3) + 15(2) + 16(2)$$
$$= 50 + 16 + 20 + 24 + 30 + 32 = 172$$

(The tree in Fig. 10-39 has path length 231.)

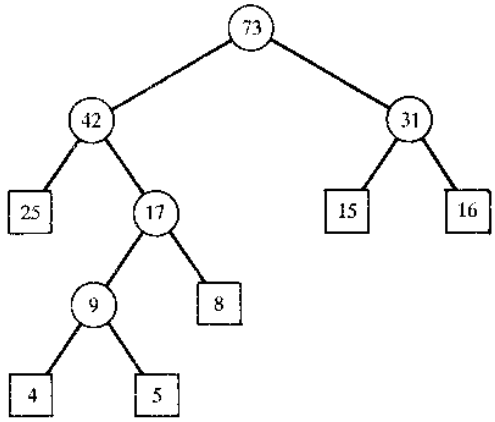


Fig. 10-40

10.16. Suppose data items A, B, C, D, E, F, G occur with the following probability distribution:

Date item:	A	B	C	D	E	F	G
Probability:	10	30	5	15	20	15	5

Find a Huffman code for the data.

Apply the Huffman algorithm to find a 2-tree T with a minimum weighted path length P as follows:

(*a*) 10, 30, 5, 15, 20, 15, 5

(*b*) 10, 30, 10*, 15, 20, 15

(*c*) 20*, 30, 15, 20, 15

(*d*) 20 30, 30*, 20

(*e*) 40*, 30, 30

(*f*) 4060*

(*g*) 100*

(Again, the circled number indicates the root of the new subtree in the step.) The tree T is drawn from Step (*g*) backward, yielding Fig. 10-41. Assign bit labels to the branches of the tree T, 0 to a left branch and 1 to a right branch, as in Fig. 10.41. The tree T yields the following Huffman code:

A: 000 *B*: 11 *C*: 0010 *D*: 100 *E*: 01 *F*: 101 *G*: 0011

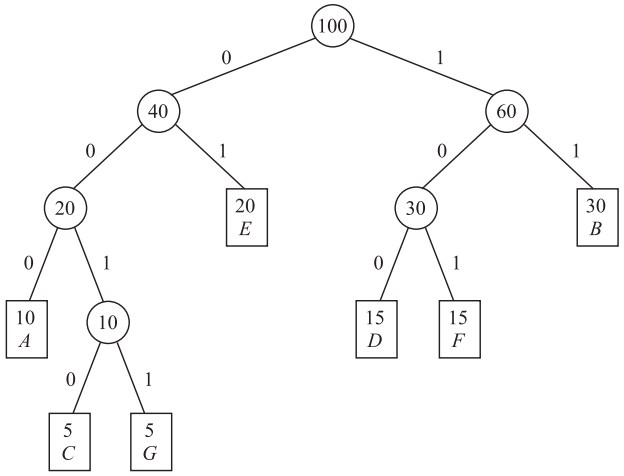


Fig. 10-41

GENERAL TREES

10.17. Consider the general tree T in Fig. 10-42(*a*). Find the corresponding binary tree T'.

The nodes of T' will be the same as the nodes of the general tree T, and in particular, the root of T' will be the same as the root of T. Furthermore, if N is a node in the binary tree T', then its left child is the first child of N in T and its right child is the next sibling of N in T. Constructing T' from the root down, we obtain the tree in Fig. 10-42(*b*).

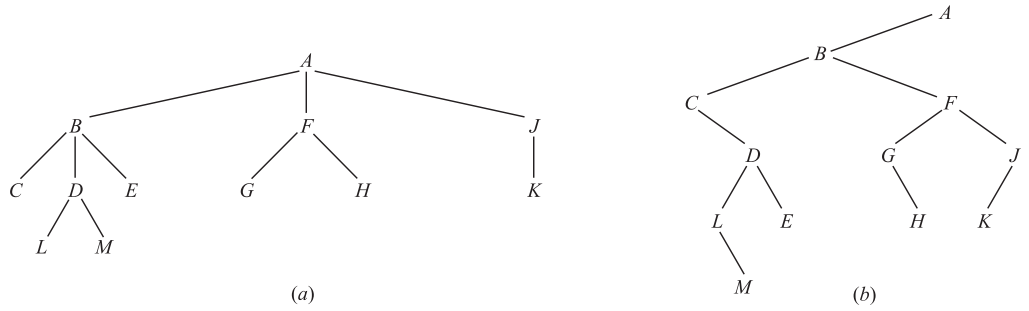


Fig. 10-42

10.18. Suppose T is a general tree with root R and subtrees $T_1, T_2, \ldots, T_M$. The preorder and postorder traversals of T are defined as follows:

Preorder: (1) Process the root R.
(2) Traverse the subtrees $T_1, T_2, \ldots, T_M$ in preorder.

Postorder: (1) Traverse the subtrees $T_1, T_2, \ldots, T_M$ in postorder.
(2) Process the root R.

Let T be the general tree in Fig. 10-42(a). Traverse T in: (a) preorder, (b) postorder.

Note that T has the root A and subtrees T_1, T_2, T_3 such that:

T_1 consists of nodes B, C, D, E, L, M.
T_2 consists of nodes F, G, H.
T_3 consists of nodes J, K.

(a) The preorder traversal of T consists of the following steps:

(i) Process root A.
(ii) Traverse T_1 in preorder: Process nodes B, C, D, L, M, E.
(iii) Traverse T_2 in preorder: Process nodes F, G, H.
(iv) Traverse T_3 in preorder: Process nodes J, K.

Accordingly, the preorder traversal of T is as follows:

$$A, \quad B, \quad C, \quad D, \quad L, \quad M, \quad E, \quad F, \quad G, \quad H, \quad J, \quad K$$

(b) The postorder traversal of T consists of the following steps:

(i) Traverse T_1 in postorder: Process nodes C, L, M, D, E, B.
(ii) Traverse T_2 in postorder: Process nodes G, H, F.
(iii) Traverse T_3 in postorder: Process nodes K, J.
(iv) Process root A.

Accordingly, the postorder traversal of T is as follows:

$$C, \quad L, \quad M, \quad D, \quad E, \quad B, \quad G, \quad H, \quad F, \quad K, \quad L, \quad A$$

10.19. Consider the binary tree T' in Fig. 10-42(b). Find the preorder, inorder, and postorder traversals of T'. Compare these traversals with the preorder and postorder traversals (which were obtained in Problem 10.18) of the corresponding general tree T in Fig. 10-42(a).

Using the binary tree traversal algorithms in Section 10.5, we obtain the following traversals of T':

Preorder:	A,	B,	C,	D,	L,	M,	E,	F,	G,	H,	J,	K
Inorder:	C,	L,	M,	D,	E,	B,	G,	H,	F,	K,	L,	A
Postorder:	M,	L,	E,	D,	C,	H,	G,	K,	J,	F,	B,	A

Observe that the preorder of the binary tree T' is identical to the preorder of the general T, and that the inorder traversal of the binary tree T' is identical to the postorder traversal of the general tree T. There is no natural traversal of the general tree T which corresponds to the postorder traversal of its corresponding binary tree T'.

Supplementary Problems

BINARY TREES

10.20. Consider the binary tree T in Fig. 10-43(a).

(a) Find: (i) depth d of T; (ii) the descendants of B.

(b) List the nodes of T in (i) preorder; (ii) inorder; (iii) postorder.

10.21. Consider the binary tree T in Fig. 10-43(a).

(a) Find the linked representation of T in memory. Assume the nodes of T are stored in a linear array INFO with 10 locations as follows:

$$\text{INFO}[1] = A, \quad \text{INFO}[2] = C, \quad \text{INFO}[3] = E, \quad \text{INFO}[4] = G$$
$$\text{INFO}[7] = B, \quad \text{INFO}[8] = D, \quad \text{INFO}[9] = F, \quad \text{INFO}[10] = H$$

(b) Find the sequential representation of T in memory.

10.22. Repeat Problems 10.20 and 10.21 for the binary tree T in Fig. 10-43(b).

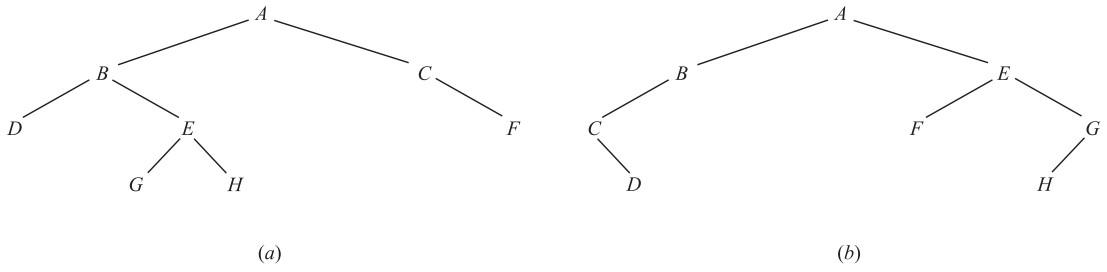


Fig. 10-43

10.23. Let T be the binary tree T stored in memory as in Fig. 10-44 where ROOT = 14.

(a) Draw the diagram of T.

(b) List the nodes of T in (i) preorder; (ii) inorder; (iii) postorder.

(c) Find the depth d of T, and find the minimum number of locations required for a linear array TREE if T were stored sequentially in TREE.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
INFO	*H*	*R*		*P*	*B*		*E*		*C*	*F*	*Q*	*S*		*A*	*K*	*L*		D
LEFT	4	0		0	18		1		0	15	0	0		5	2	0		0
RIGHT	11	0		0	7		0		10	16	12	0		9	0	0		0

Fig. 10-44

10.24. Suppose the preorder and inorder traversals of a binary tree T yield the following sequence of nodes:

Preorder: *G*, *B*, *Q*, *A*, *C*, *K*, *F*, *P*, *D*, *E*, *R*, *H*

Inorder: *Q*, *B*, *K*, *C*, *F*, *A*, *G*, *P*, *E*, *D*, *H*, *R*

(*a*) Draw the diagram of T.

(*b*) Find: (i) depth d of T; (ii) the decendants of *B*.

(*c*) List the terminal nodes of T.

10.25. Draw the 2-tree T which corresponds to the algebraic expression $E = (x + 3y)^4(a - 2b)$, and find the preorder of T.

BINARY SEARCH TREES, HEAPS

10.26. Draw the final tree T if the following numbers are inserted into an empty binary search tree T:

50, 33, 44, 22, 77, 35, 60, 40

10.27. Consider the binary search tree T in Fig. 10-45. Suppose nodes 20, 55, 88 are added one after the other to T. Find the final tree T.

10.28. Consider the binary search tree T in Fig. 10-45. Suppose nodes 22, 25, 75 are deleted one after the other from T. Find the final tree T.

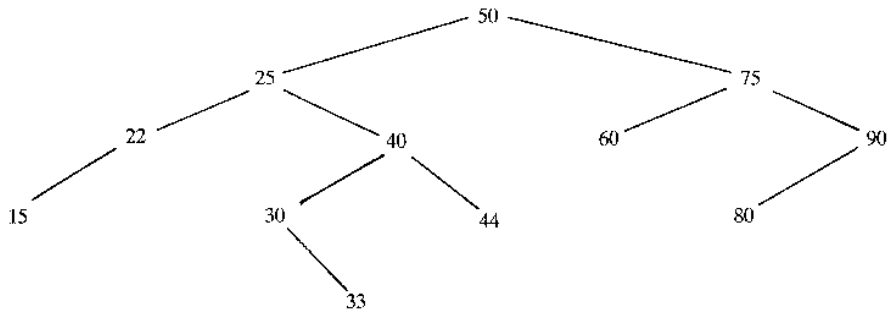


Fig. 10-45

10.29. Consider the complete tree T with $N = 10$ nodes in Fig. 10-46.

(*a*) Find the sequential representation of T in an array A in memory.

(*b*) Form a maxheap H out of T by repeatedly inserting $A[J + 1]$ into the heap $A[1]$ to $A[J]$ (as was done in Problem 10.13).

(*c*) Form a minheap H' (instead of a maxheap) out of T.

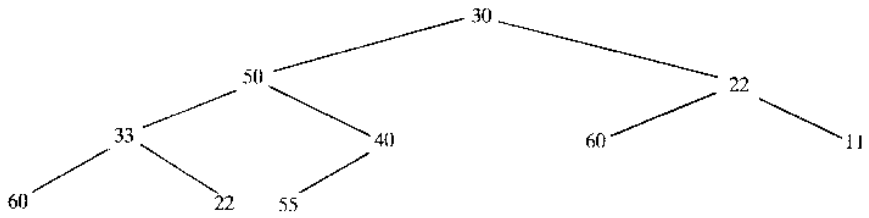


Fig. 10-46

HUFFMAN ALGORITHM, GENERAL TREES

10.30. Consider the 2-tree T in Fig. 10-47 which contains the seven letters A, B, C, D, E, F, G as external nodes. Find the Huffman coding of the letters determined by the tree T.

10.31. Suppose the seven data items $A, B, \ldots, G$ are assigned the following weights:

$$(A, 13), \quad (B, 2), \quad (C, 19), \quad (D, 23), \quad (E, 29), \quad (F, 5), \quad (G, 9)$$

Find the weighted path length P of the tree in Fig. 10-47.

10.32. Using the data in Problem 10.31, find a Huffman coding for the seven letters using a 2-tree with a minimum weighted path length P, and find P.

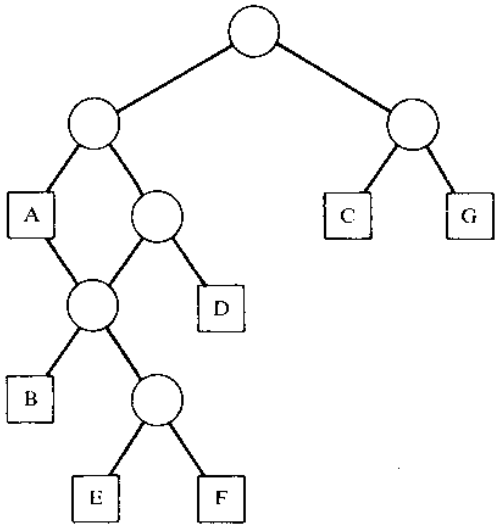


Fig. 10-47

10.33. Consider the forest F in Fig. 10-48 which consists of three trees with roots A, B, and C, respectively. Draw the binary tree F' corresponding to F.

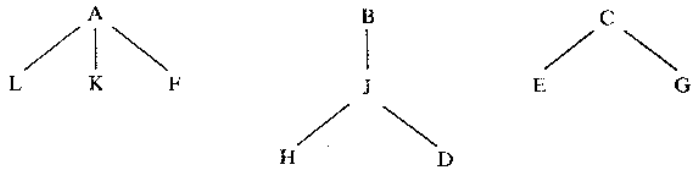


Fig. 10-48

COMPUTER PROBLEMS

Problems 10.34 to 10.39 refer to Figure 10-49 which is a list of employee records stored in memory. It is a binary search tree with respect to the NAME key. It also uses a header node which lists the number of employees in SSN[HEAD] and the total salary in SALARY[HEAD]. Also, to allow insertions, the available (empty) locations form a linked list with AVAIL pointing to the first element in the list and the linking is maintained by the array LEFT.

HEAD 5

AVAIL 8

	NAME	SSN	SEX	SALARY	LEFT	RIGHT
1					0	
2	Davis	192-38-7282	Female	22 800	5	12
3	Kelly	165-64-3351	Male	19 000	5	5
4	Green	175-56-2251	Male	27 200	2	5
5		009		191 600	14	5
6	Brown	178-52-1065	Female	14 700	5	5
7	Lewis	181-58-9939	Female	16 400	3	10
8					11	
9	Cohen	177-44-4557	Male	19 000	6	4
10	Rubin	135-46-6262	Female	15 500	5	5
11					13	
12	Evans	168-56-8113	Male	34 200	5	5
13					1	
14	Harris	208-56-1654	Female	22 800	9	7

Fig. 10-49

10.34. Write a program which prints the list of employee records in alphabetical order. (*Hint*: Print the records in inorder.)

10.35. Write a program which reads the name *NNN* of an employee and prints the employee's record. Test the program using (*a*) Evans, (*b*) Smith, and (*c*) Lewis.

10.36. Write a program which reads the social security number *SSS* of an employee and prints the employee's record. Test the program using (*a*) 165-64-3351, (*b*) 135-46-6262, and (*c*) 177-44-5555.

10.37. Write a program which reads an integer K and prints the name of each male employee when $K = 1$ or of each female employee when $K = 2$. Test the program using (*a*) $K = 2$, (*b*) $K = 5$, and (*c*) $K = 1$.

10.38. Write a program which reads the name *NNN* of an employee and deletes the employee's record from the structure. Test the program using (*a*) Davis, (*b*) Jones, and (*c*) Rubin.

10.39. Write a program which reads the record of a new employee and inserts the record into the file. Test the program using:

(*a*) Fletcher; 168-52-3388; Female; 21 000.

(*b*) Nelson; 175-32-2468; Male; 19 000.

Answers to Supplementary Problems

10.20. (*a*) (i) $d = 4$; (ii) D, E, G, H.
(*b*) (i) $ABDEGHCF$; (ii) $DBGEHACF$; (iii) $DGHEBFCA$.

10.21. See: (*a*) Fig. 10-50(*a*); (*b*) Fig. 10-51(*a*) where END = 11.

10.22. (*a*) (i) $d = 4$; (ii) C, D.
(*b*) (i) $ABCDEFGH$; (ii) $CDBAFEHG$; (iii) $DCBFHGEA$.

Also, see Fig. 10-50(*a*) and Fig. 10-51(*b*) where END = 14.

	1	2	3	4	5	6	7	8	9	10
INFO	*A*	*C*	*E*	*G*			*B*	*D*	*F*	*H*
LEFT	7	0	4	0			8	0	0	0
RIGHT	2	9	10	0			3	0	0	0

(*a*)

	1	2	3	4	5	6	7	8	9	10
INFO	*A*	*C*	*E*	*G*			*B*	*D*	*F*	*H*
LEFT	7	0	9	10			2	0	0	0
RIGHT	2	8	4	0			3	0	0	0

(*b*)

Fig. 10-50

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
(*a*) TREE	*A*	*B*	*C*	*D*	*E*		*F*			*G*	*H*					
(*b*) TREE	*A*	*B*	*E*	*C*		*F*	*G*		*D*					*H*		

Fig. 10-51

10.23. (*a*) See Fig. 10-52.
(*b*) (i) $ABDEHPQSCFKRL$; (ii) $DBPHQSEACRKFL$; (iii) $DPSQHEBRKLFCA$.
(*c*) $d = 6$; hence $32 \leq \text{END} < 64$. Specifically, END = 43.

10.24. (*a*) See Fig. 10-53.
(*b*) (i) $d = 5$; (ii) Q, A, C, K, F.
(*c*) Q, K, F, E, H

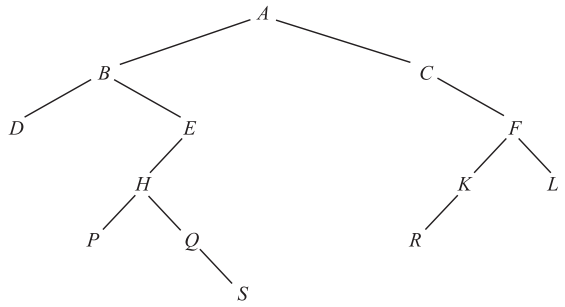


Fig. 10-52

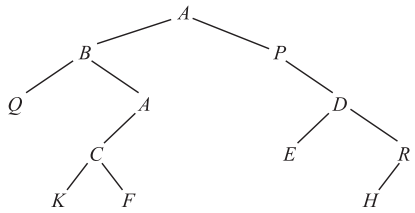


Fig. 10-53

10.25. See Fig. 10-54. Preorder: $* \uparrow + x * 3\, y\, 4 - a\, 2 * b$.

10.26. See Fig. 10-55.

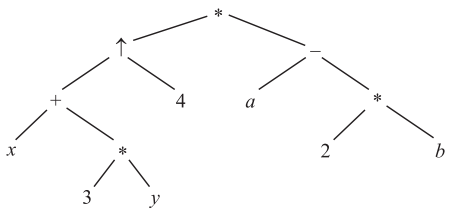


Fig. 10-54

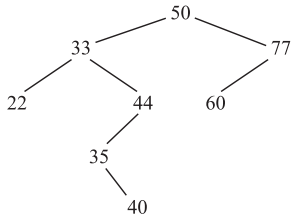


Fig. 10-55

10.27. See Fig. 10-56.

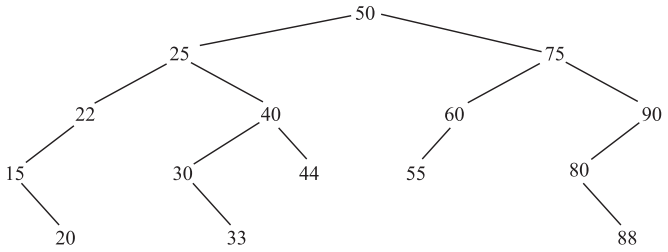


Fig. 10-56

10.28. See Fig. 10-57.

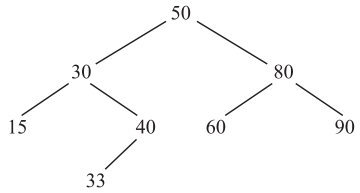


Fig. 10-57

10.29. (*a*) TREE: 30, 50, 22, 33, 40, 60, 11, 60, 22, 55.
(*b*) See Fig. 10-58(*a*).
(*c*) See Fig. 10-58(*b*).

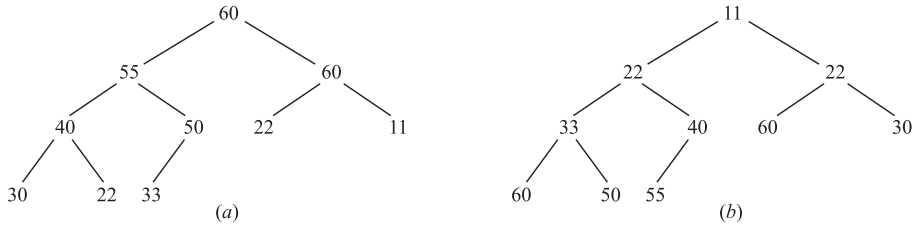


Fig. 10-58

10.30. *A*:00; *B*:0100; *C*:10; *D*:011; *E*:01010; *F*:01011; *G*:11.

10.31. $P = 329$.

10.32. *A*:000; *B*:00101; *C*:10; *D*:11; *E*:01; *F*:00100; *G*:0011; $P = 257$.

10.33. See Fig. 10-59.

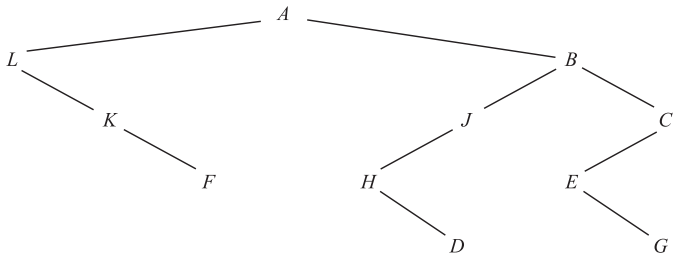


Fig. 10-59

© The McGraw–Hill Companies, 2004

Chapter 11

Properties of the Integers

11.1 INTRODUCTION

This chapter investigates some basic properties of the *natural numbers* (or *positive integers*), that is, the set

$$\mathbf{N} = \{1, 2, 3, \ldots\}$$

and their "cousins", the integers, that is, the set

$$\mathbf{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$$

(The letter **Z** comes from the word "Zahlen" which means numbers in German.)

The following simple rules concerning the addition and multiplication of these numbers are assumed:

(*a*) Associative law for multiplication and addition:

$$(a + b) + c = a + (b + c) \qquad \text{and} \qquad (ab)c = a(bc)$$

(*b*) Commutative law for multiplication and addition:

$$a + b = b + a \qquad \text{and} \qquad ab = ba$$

(*c*) Distributive law:

$$a(b + c) = ab + ac$$

(*d*) Additive identity 0 and multiplicative identity 1:

$$a + 0 = 0 + a = a \qquad \text{and} \qquad a \cdot 1 = 1 \cdot a = a$$

(*e*) Additive inverse $-a$ for any integer a:

$$a + (-a) = (-a) + a = 0$$

The next chapter shows that other mathematical structures have the above properties. One fundamental property which distinguishes the integers **Z** from other structures is the Principle of Mathematical Induction (Section 1.10) which we rediscuss here. We also state and prove (Problem 11.34) the following theorem.

Fundamental Theorem of Arithmetic: Every positive integer $n > 1$ can be written uniquely as a product of prime numbers.

This theorem already appeared in Euclid's *Elements*. Here we also develop the concepts and methods which are used to prove this important theorem.

11.2 ORDER AND INEQUALITIES, ABSOLUTE VALUE

This section discusses the elementary properties of order and absolute value.

Order

Let a and b be integers. We say a is *less than* b, written

$$a < b$$

if the difference $b - a$ is positive, that is, if $b - a$ belongs to **N**.

Observe that we define order in **Z** in terms of the positive integers **N**. All the usual properties of this order relation are a consequence of the following two properties of **N**:

[$\mathbf{P}_1$] If a and b belong to **N**, then $a + b$ and ab belong to **N**.

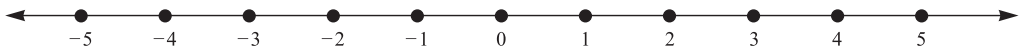
[$\mathbf{P}_2$] For any integer a, either $a \in \mathbf{N}$, $a = 0$, or $-a \in \mathbf{N}$.

The following notation is also used:

$a > b$, means $b < a$;	read: a is greater than b.
$a \leq b$, means $a < b$ or $a = b$;	read: a is less than or equal to b.
$a \geq b$, means $b \leq a$;	read: a is greater than or equal to b.

The relations $<$, $>$, $\leq$ and $\geq$ are called *inequalities* in order to distinguish them from the relation $=$ of equality.

The reader is certainly familiar with the representation of the integers as points on a straight line, called the *number line* **R**, as follows:



We note that $a < b$ if and only if a lies to the left of b on the above number line. For example,

$$2 < 5; \quad -6 < -3; \quad 4 \leq 4; \quad 5 > -8; \quad 6 \geq 0; \quad -7 \leq 0$$

We also note that a is positive iff $a > 0$, and a is negative iff $a < 0$. (Recall "iff" means "if and only if".)

Basic properties of the inequality relations follow.

Proposition 11.1: The relation $\leq$ in **Z** has the following properties:
(i) $a \leq a$, for any integer a.
(ii) If $a \leq b$ and $b \leq a$, then $a = b$.
(iii) If $a \leq b$ and $b \leq c$, than $a \leq c$.

Proposition 11.2: **(Law of Trichotomy):** For any integers a and b, exactly one of the following holds:

$$a < b, \qquad a = b, \qquad \text{or} \qquad a > b$$

Proposition 11.3: Suppose $a \leq b$, and let c be any integer. Then:
(i) $a + c \leq b + c$.
(ii) $ac \leq bc$ when $c > 0$; but $ac \geq bc$ when $c < 0$.

(Problem 11.6 proves Proposition 11.3.)

Absolute Value

The *absolute value* of an integer a, written $|a|$, is formally defined by:

$$|a| = \begin{cases} a, & \text{if } a \geq 0 \\ -a, & \text{if } a < 0 \end{cases}$$

Accordingly, $|a| > 0$ except when $a = 0$. Geometrically speaking, $|a|$ may be viewed as the distance between the points a and 0. Also, $|a - b| = |b - a|$ may be viewed as the distance between the points a and b. For example:

(*a*) $|-3| = 3$; $|7| = 7$; $|-13| = 13$
(*b*) $|2 - 7| = |-5| = 5$ and $|7 - 2| = |5| = 5$
(*c*) $|-3 - 8| = |-11| = 11$

Some properties of the absolute value function follow. [Problems 11.7 and 8 prove (iii) and (iv).]

Proposition 11.4: Let a and b be any integers. Then:

(i) $|a| \geq 0$, and $|a| = 0$ iff $a = 0$.

(ii) $-|a| \leq a \leq |a|$.

(iii) $|ab| = |a|\ |b|$.

(iv) $|a \pm b| \leq |a| + |b|$.

(v) $|\ |a| - |b|\ | \leq |a \pm b|$.

11.3 MATHEMATICAL INDUCTION

The principle of mathematical induction stated below essentially asserts that the positive integers **N** begin with the number 1 and the rest are obtained by successively adding 1. That is, we begin with 1, then $2 = 1 + 1$, then $3 = 2 + 1$, then $4 = 3 + 1$, and so on. The principle makes precise the vague phrase "and so on".

Principle of Mathematical Induction: Let S be a set of positive integers with the following two properties:

(i) 1 belongs to S.

(ii) If k belongs to S, then $k + 1$ belongs to S.

Then S is the set of all positive integers.

We shall not prove this principle. On the contrary, when the set **N** of positive integers (natural numbers) is developed axiomatically, this principle is given as one of the axioms.

There is an equivalent form of the above principle which is usually used when proving theorems:

Principle of Mathematical Induction: Let P be a proposition defined on the integers $n \geq 1$ such that:

(i) $P(1)$ is true.

(ii) $P(n + 1)$ is true whenever $P(n)$ is true.

Then P is true for every integer $n \geq 1$.

EXAMPLE 11.1

(*a*) Let P be the proposition that the sum of the first n odd numbers is n^2; that is:

$$P(n): \quad 1 + 3 + 5 + \cdots + (2n - 1) = n^2$$

(The nth odd number is $2n - 1$ and the next odd number is $2n + 1$.) $P(n)$ is clearly true for $n = 1$; that is:

$$P(1): \quad 1 = 1^2$$

Suppose $P(n)$ is true. (This is called the inductive hypothesis.) Adding $2n + 1$ to both sides of $P(n)$ we obtain

$$\begin{aligned} 1 + 3 + 5 + \cdots + (2n - 1) + (2n + 1) &= n^2 + (2n + 1) \\ &= (n + 1)^2 \end{aligned}$$

which is $P(n + 1)$. We have shown that $P(n + 1)$ is true whenever $P(n)$ is true. By the principle of mathematical induction, P is true for all n.

(*b*) The symbol $n!$ (read: n factorial) is defined as the product of the first n positive integers, that is,

$$1! = 1, \qquad 2! = 1 \cdot 2 = 2, \qquad 3! = 1 \cdot 2 \cdot 3 = 6, \qquad \text{and so on}$$

This may be formally defined as follows:

$$1! = 1 \quad \text{and} \quad (n + 1)! = (n + 1)(n!) \text{ for } n > 1$$

Observe that if S is the set of positive integers for which ! is defined, then S satisfies the two properties of mathematical induction. Hence the above definition defines ! for every positive integer.

There is another form of the principle of mathematical induction (proved in Problem 11.15) which is sometimes more convenient to use. Namely:

Theorem 11.5 (Induction: Second Form): Let P be a proposition which is defined on the integers $n \geq 1$ such that:

(i) $P(1)$ is true.

(ii) $P(n)$ is true whenever $P(k)$ is true for all $1 \leq k < n$.

Then P is true for every integer $n \geq 1$.

Remark: The above theorem is true if we replace 1 by 0 or by any other integer m.

Well-Ordering Principle

A property of the positive integers which is equivalent to the principle of induction, although apparently very dissimilar, is the well-ordering principle (proved in Problem 11.14). Namely:

Theorem 11.6 (Well-Ordering Principle): Let S be a nonempty set of positive integers. Then S contains a *least element*; that is, S contains an element a such that $a \leq s$ for every s in S.

Generally speaking, an ordered set S is said to be *well ordered* if every subset of S contains a first element. Thus Theorem 11.6 states that **N** is well ordered.

A set S of integers is said to be *bounded from below* if every element of S is greater than some integer m (which may be negative). (The number m is called a *lower bound* of S.) A simple corollary of the above theorem follows:

Corollary 11.7: Let S be a nonempty set of integers which is bounded from below. Then S contains a least element.

11.4 DIVISION ALGORITHM

The following fundamental property of arithmetic (proved in Problems 11.20 and 11.21) is essentially a restatement of the result of long division.

Theorem 11.7 (Division Algorithm): Let a and b be integers with $b \neq 0$. Then there exists integers q and r such that

$$a = bq + r \qquad \text{and} \qquad 0 \leq r < |b|.$$

Also, the integers q and r are unique.

The number q in the above theorem is called the *quotient*, and r is called the *remainder*. We stress the fact that r must be nonnegative. The theorem also states that

$$a - bq = r$$

This equation will be used subsequently.

If a and b are positive, then q is nonnegative. If b is positive, then Fig. 11-1 gives a geometrical interpretation of this theorem. That is, the positive and negative multiples of b will be evenly distributed throughout the number line **R**, and a will fall between some multiples qb and $(q+1)b$. The distance between qb and a is then the remainder r.

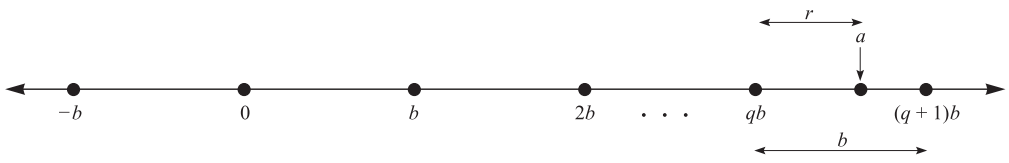


Fig. 11-1

EXAMPLE 11.2

(*a*) Let $a = 4461$ and $b = 16$. We find $q = 278$ and $r = 13$, by by long division, say, as in Fig. 11-2(*a*). As expected,

$$4461 = 16(278) + 13$$

That is, $a = bq + r$.

(*b*) Let $a = -262$ and $b = 3$. First we divide 262 by 3, say, as in Fig. 11-2(*b*). This yields a quotient 87 and remainder 1; hence

$$262 = 3(87) + 1$$

We need $a = -262$, so we multiply by -1 obtaining

$$-262 = 3(-87) - 1$$

However, -1 is negative and hence cannot be r. We correct this by adding and subtracting the value of b (which is 3) as follows:

$$-262 = 3(-87) - 3 + 3 - 1 = 3(-88) + 2$$

Therefore, $q = -88$ and $r = 2$.

(*c*) Let $b = 2$. Then any integer a can be written in the form

$$a = 2q + r \qquad \text{and} \qquad 0 \le r < 2$$

Thus r can only be 0 or 1. Thus every integer is of the form $2k$ or $2k + 1$. The integers of the form $2k$ are called *even* integers, while those of the form $2k + 1$ are called *odd* integers. (Usually, an even integer is defined as an integer divisible by 2, and all other integers are said to be odd. Thus the division algorithm proves that every odd integer has the form $2k + 1$.)

$$\begin{array}{r} 278 \\ 16\overline{)4461} \\ \underline{32} \\ 126 \\ \underline{112} \\ 141 \\ \underline{128} \\ 13 \end{array}$$

(*a*)

$$\begin{array}{r} 87 \\ 3\overline{)262} \\ \underline{24} \\ 22 \\ \underline{21} \\ 1 \end{array}$$

(*b*)

Fig. 11-2

11.5 DIVISIBILITY, PRIMES

Let a and b be integers with $a \neq 0$. Suppose $ac = b$ for some integer c. We then say that *a divides b* or b is *divisible* by a and write

$$a|b$$

We may also say that b is a *multiple* of a or that a is a *factor* or *divisor* of b. If a does not divide b, we will write $a \nmid b$.

EXAMPLE 11.3

(*a*) $3|6$ since $3 \cdot 2 = 6$; and $-4|28$ since $(-4)(-7) = 28$.

(*b*) The divisors:

(i) of 1 are ± 1;
(ii) of 2 are ± 1, ± 2;
(iii) of 4 are ± 1, ± 2, ± 4;
(iv) of 5 are ± 1 ± 5;
(v) of 7 are ± 1, ± 7;
(vi) of 9 are ± 1, ± 3, ± 9.

(*c*) If $a \neq 0$, then $a|0$ since $a \cdot 0 = 0$.

(*d*) Every integer a is divisible by ± 1 and $\pm a$. These are sometimes called the *trivial divisors* of a.

The basic properties of divisibility is stated in the next theorem (proved in Problem 11.28).

Theorem 11.8: Suppose a, b, c are integers.
(i) If $a|b$ and $b|c$, then $a|c$.
(ii) If $a|b$ then, for any integer x, $a|bx$.
(iii) If $a|b$ and $a|c$, then $a|(b + c)$ and $a|(b - c)$.
(iv) If $a|b$ and $b \neq 0$, then $a = \pm b$ or $|a| < |b|$.
(v) If $a|b$ and $b|a$, then $|a| = |b|$, i.e., $a = \pm b$.
(vi) If $a|1$, then $a = \pm 1$.

Putting (ii) and (iii) together, we obtain the following important result.

Corollary 11.9: Supose $a|b$ and $a|c$. Then, for any integers x and y, $a|(bx + cy)$.

The expression $bx + cy$ will be called a *linear combination* of b and c.

Primes

A positive integer $p > 1$ is called a *prime number* or a *prime* if its only divisors are ± 1 and $\pm p$, that is, if p only has trivial divisors. If $n > 1$ is not prime, then n is said to be *composite*. We note (Problem 11.13) that if $n > 1$ is composite then $n = ab$ where $1 < a, b < n$.

EXAMPLE 11.4

(*a*) The integers 2 and 7 are primes, whereas $6 = 2 \cdot 3$ and $15 = 3 \cdot 5$ are composite.

(*b*) The primes less than 50 follow.

$$2, \quad 3, \quad 5, \quad 7, \quad 11, \quad 13, \quad 17, \quad 19, \quad 23, \quad 29, \quad 31, \quad 37, \quad 41, \quad 43, \quad 47$$

(*c*) Although 21, 24, and 1729 are not primes, each can be written as a product of primes:

$$21 = 3 \cdot 7, \qquad 24 = 2 \cdot 2 \cdot 2 \cdot 3 = 2^3 \cdot 3, \qquad 1729 = 7 \cdot 13 \cdot 19$$

The Fundamental Theorem of Arithmetic states that every integer $n > 1$ can be written as a product of primes in essentially one way; it is a deep and somewhat difficult theorem to prove. However, using induction, it is easy at this point to prove that such a product exists. Namely:

Theorem 11.10: Every integer $n > 1$ can be written as a product of primes.

Note that a product may consist of a single factor so that a prime p is itself a product of primes. We prove Theorem 11.10 here, since its proof is relatively simple.

Proof: The proof is by induction. Let $n = 2$. Since 2 is prime, n is a product of primes. Suppose $n > 2$, and the theorem holds for positive integers less than n. If n is prime, then n is a product of primes. If n is composite, then $n = ab$ where $a, b < n$. By induction, a and b are products of primes; hence $n = ab$ is also a product of primes.

Euclid, who proved the Fundamental Theorem of Arithmetic, also asked whether or not there was a largest prime. He answered the question thusly:

Theorem 11.11: There is no largest prime, that is, there exists an infinite number of primes.

Proof: Suppose there is a finite number of primes, say $p_1, p_2, \ldots, p_m$. Consider the integer

$$n = p_1 p_2 \cdots p_m + 1$$

Since n is a product of primes (Theorem 11.10), it is divisible by one of the primes, say p_k. Note that p_k also divides the product $p_1 p_2 \cdots p_m$. Therefore p_k divides

$$n - p_1 p_2 \cdots p_m = 1$$

This is impossible, and so n is divisible by some other prime. This contradicts the assumption that $p_1, p_2, \ldots, p_m$ are the only primes. Thus the number of primes is infinite, and the theorem is proved.

11.6 GREATEST COMMON DIVISOR, EUCLIDEAN ALGORITHM

Suppose a and b are integers, not both 0. An integer d is called a *common divisor* of a and b if d divides both a and b, that is, if $d|a$ and $d|b$. Note that 1 is a positive common divisor of a and b, and that any common divisor of a and b cannot be greater than $|a|$ or $|b|$. Thus there exists a largest common divisor of a and b; it is denoted by

$$\gcd(a, b)$$

and it is called the *greatest common divisor* of a and b.

EXAMPLE 11.5

(a) The common divisors of 12 and 18 are ± 1, ± 2, ± 3, ± 6. Thus

$$\gcd(12, 18) = 6$$

Similarly,

$$\gcd(12, -18) = 6, \qquad \gcd(12, -16) = 4, \qquad \gcd(29, 15) = 1, \qquad \gcd(14, 49) = 7$$

(b) For any integer a, we have $\gcd(1, a) = 1$.

(c) For any prime p, we have

$$\gcd(p, a) = p \quad \text{or} \quad \gcd(p, a) = 1$$

according as $p|a$ or $p \nmid a$.

(d) Suppose a is positive. Then $a|b$ if and only if $\gcd(a, b) = a$.

The following theorem (proved in Problem 11.30) gives an alternative characterization of the greatest common divisor.

Theorem 11.12: Let d be the smallest positive integer of the form $ax + by$. Then $d = \gcd(a, b)$.

Corollary 11.13: Suppose $d = \gcd(a, b)$. Then there exists integers x and y such that $d = ax + by$.

Another way to characterize the greatest common divisor, without using the inequality relation, follows:

Theorem 11.14: A positive integer $d = \gcd(a, b)$ if and only if d has the following two properties:
(1) d divides both a and b.
(2) If c divides both a and b, then $c|d$.

Simple properties of the greatest common divisor follow.

(*a*) $\gcd(a, b) = \gcd(b, a)$.

(*b*) If $x > 0$, then $\gcd(ax, bx) = x \cdot \gcd(a, b)$.

(*c*) If $d = \gcd(a, b)$, then $\gcd(a/d, b/d) = 1$.

(*d*) For any integer x, $\gcd(a, b) = \gcd(a, b + ax)$.

Euclidean Algorithm

Let a and b be integers, and let $d = \gcd(a, b)$. One can always find d by listing all the divisors of a and then all the divisors of b and then choosing the largest common divisor. Letting $n = |a| + |b|$ and counting the number of divisions, the complexity of such an algorithm is $f(n) = O(\sqrt{n})$. Also, we have given no method to find the integers x and y such that

$$d = ax + by$$

This subsection gives a very efficient algorithm with complexity $f(n) = O(\log n)$ for finding both $d = \gcd(a, b)$ and the above integers x and y.

This algorithm, called the Euclidean Algorithm, consists of repeatedly applying the division algorithm (long division). We illustrate the algorithm with an example.

EXAMPLE 11.6 Let $a = 540$ and $b = 168$. We find $d = \gcd(a, b)$ by dividing a by b and then repeatedly dividing each remainder into the divisor until obtaining a zero remainder. These steps are pictured in Fig. 11-3. The last nonzero remainder is 12. Thus

$$12 = \gcd(540, 168)$$

This follows from the fact that

$$\gcd(540, 168) = \gcd(168, 36) = \gcd(36, 24) = \gcd(24, 12) = 12$$

$$\begin{array}{r} 3 \\ 168\overline{)540} \\ \uparrow\ \underline{504} \\ \quad 36 \end{array} \qquad \begin{array}{r} 4 \\ 36\overline{)168} \\ \uparrow\ \underline{144} \\ \quad 24 \end{array} \qquad \begin{array}{r} 1 \\ 24\overline{)36} \\ \uparrow\ \underline{24} \\ \quad 12 \end{array} \qquad \begin{array}{r} 2 \\ 12\overline{)24} \\ \underline{24} \\ 0 \end{array}$$

Fig. 11-3

Next we find x and y such that

$$12 = 540x + 168y$$

The first three quotients in Fig. 11-3 yield the equations:

$$\begin{array}{lllll} (1) & 540 = 3(168) + 36 & \text{or} & 36 = 540 - 3(168) \\ (2) & 168 = 4(36) + 24 & \text{or} & 24 = 168 - 4(36) \\ (3) & 36 = 1(24) + 12 & \text{or} & 12 = 36 - 1(24) \end{array}$$

Equation (*3*) tells us that 12 is a linear combination of 36 and 24. We use (*2*) to replace 24 in (*3*) so we can write 12 as a linear combination of 168 and 36 as follows:

$$\begin{aligned} (4) \quad 12 &= 36 - 1[168 - 4(36)] = 36 - 1(168) + 4(36) \\ &= 5(36) - 1(168) \end{aligned}$$

We now use (*1*) in (*4*) so we can write 12 as a linear combination of 168 and 540 as follows:

$$\begin{aligned} 12 &= 5[540 - 3(168)] - 1(168) \\ &= 5(54) - 15(168) - 1(168) \\ &= 5(540) - 16(168) \end{aligned}$$

This is our desired linear combination. Thus $x = 5$ and $y = -16$.

Least Common Multiple

Suppose a and b are nonzero integers. Note that $|ab|$ is a positive common multiple of a and b. Thus there exists a smallest positive common multiple of a and b; it is denoted by

$$\text{lcm}\,(a, b)$$

and it is called the *least common multiple* of a and b.

EXAMPLE 11.7

(a) $\text{lcm}\,(2, 3) = 6$; $\text{lcm}\,(4, 6) = 12$; $\text{lcm}\,(9, 10) = 90$.

(b) For any positive integer a, we have $\text{lcm}\,(1, a) = a$.

(c) For any prime p and any positive integer a,

$$\text{lcm}\,(p, a) = a \qquad \text{or} \qquad \text{lcm}\,(p, a) = ap$$

according as $p|a$ or $p \nmid a$.

(d) Suppose a and b are positive integers. Then $a|b$ if and only if $\text{lcm}\,(a, b) = b$.

The next theorem gives an important relationship between the greatest common divisor and the least common multiple.

Theorem 11.15: Suppose a and b are nonzero integers. Then

$$\text{lcm}\,(a, b) = \frac{|ab|}{\text{gcd}\,(a, b)}$$

11.7 FUNDAMENTAL THEOREM OF ARITHMETIC

This section discusses the Fundamental Theorem of Arithmetic. First we need the notion of relatively prime integers.

Relatively Prime Integers

Two integers a and b are said to be *relatively prime* or *coprime* if

$$\text{gcd}\,(a, b) = 1$$

Accordingly, if a and b are relatively prime, then there exist integers x and y such that

$$ax + by = 1$$

Conversely, if $ax + by = 1$, then a and b are relatively prime.

EXAMPLE 11.8

(a) Observe that:

$$\text{gcd}\,(12, 35) = 1, \qquad \text{gcd}\,(49, 18) = 1, \qquad \text{gcd}\,(21, 64) = 1, \qquad \text{gcd}\,(-28, 45) = 1$$

(b) If p and q are distinct primes, then $\text{gcd}\,(p, q) = 1$.

(c) For any integer a, we have

$$\text{gcd}\,(a, a + 1) = 1$$

This follows from the fact that any common divisor of a and $a + 1$ must divide their difference $(a + 1) - a = 1$.

The relation of being relatively prime is particularly important because of the following results. We will prove the second theorem here.

Theorem 11.16: Suppose $\gcd(a, b) = 1$, and a and b both divide c. The ab divides c.

Theorem 11.17: Suppose $a|bc$, and $\gcd(a, b) = 1$. Then $a|c$.

Proof: Since $\gcd(a, b) = 1$, there exist x and y such that $ax + by = 1$. Multiplying by c yields

$$acx + bcy = c$$

We have $a|acx$. Also, $a|bcy$ since, by hypothesis, $a|bc$. Hence a divides the sum $acx + bcy = c$.

Corollary 11.18: Suppose a prime p divides a product ab. Then $p|a$ or $p|b$.

This corollary dates back to Euclid. In fact, it is the basis of his proof of the Fundamental Theorem of Arithmetic.

Fundamental Theorem of Arithmetic

Theorem 11.10 asserts that every positive integer is a product of primes. Can different products of primes yield the same number? Clearly, we can rearrange the order of the prime factors, e.g.,

$$30 = 2 \cdot 3 \cdot 5 = 5 \cdot 2 \cdot 3 = 3 \cdot 2 \cdot 5$$

The Fundamental Theorem of Arithmetic (proved in Problem 11.35) says that this is the only way that two "different" products can give the same number. Namely:

Theorem 11.19 (Fundamental Theorem of Arithmetic): Every integer $n > 1$ can be expressed uniquely (except for order) as a product of primes.

The primes in the factorization of n need not be distinct. Frequently, it is useful to collect together all equal primes. Then n can be expressed uniquely in the form

$$n = p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r}$$

where the m_i are positive and $p_1 < p_2 < \cdots < p_r$. This is called the *canonical factorization* of n.

EXAMPLE 11.9 Let $a = 2^4 \cdot 3^3 \cdot 7 \cdot 11 \cdot 13$ and $b = 2^3 \cdot 3^2 \cdot 5^2 \cdot 11 \cdot 17$. Find $d = \gcd(a, b)$ and $m = \text{lcm}(a, b)$.

(*a*) First we find $d = \gcd(a, b)$. Those primes p_i which appear in both a and b, i.e., 2, 3, and 11, will also appear in d, and the exponent of p_i in d will be the smaller of its exponents in a and b. Thus

$$d = \gcd(a, b) = 2^3 \cdot 3^2 \cdot 11 = 792$$

(*b*) Next we find $m = \text{lcm}(a, b)$. Those primes p_i which appear in either a and b, i.e., 2, 3, 5, 7, 11, 13, and 17 will also appear in m, and the exponent of p_i in m will be the larger of its exponents in a and b. Thus

$$m = \text{lcm}(a, b) = 2^4 \cdot 3^3 \cdot 5^2 \cdot 11 \cdot 13 \cdot 17$$

We are so used to using numbers as if the Fundamental Theorem of Arithmetic were true that it may seem as if it needs no proof. It is a tribute to Euclid, who first proved the theorem, that he recognized that it does require proof. We emphasize the nontriviality of the theorem by giving an example of a system of numbers which does not satisfy this theorem.

EXAMPLE 11.10 Let F be the set of positive integers of the form $3x + 1$. Thus F consists of the numbers

$$1, \quad 4, \quad 7, \quad 10, \quad 13, \quad 16, \quad 19, \quad 22, \ldots$$

Note that the product of two numbers in F is again in F since

$$(3x + 1)(3y + 1) = 9xy + 3x + 3y + 1 = 3(3xy + x + y) + 1$$

Our definition of primes makes perfectly good sense in F. The first few primes in F are:

$$4, \quad 7, \quad 10, \quad 13, \quad 19, \quad 22, \quad 25, \ldots$$

Although $4 = 2 \cdot 2$, the number 2 is not in F. Thus 4 is prime in F since 4 has no factors except 1 and 4. Similarly 10, 22, 25, ... are primes in F. Note $100 = 3(33) + 1$ belongs to F. However, 100 has two essentially different factorizations into primes of F; namely,

$$100 = 4 \cdot 25 \qquad \text{and} \qquad 100 = 10 \cdot 10$$

Thus there is no unique factorization into primes in F.

11.8 CONGRUENCE RELATION

Let m be a positive integer. We say that a is *congruent* to b *modulo* m, written

$$a \equiv b \text{ (modulo } m) \qquad \text{or simply} \qquad a \equiv b \text{ (mod } m)$$

if m divides the difference $a - b$. The integer m is called the *modulus*. The negation of $a \equiv b \pmod m$ is written $a \not\equiv b \pmod m$. For example:

(i) $87 \equiv 23 \pmod 4$ since 4 divides $87 - 23 = 64$.

(ii) $67 \equiv 1 \pmod 6$ since 6 divides $67 - 1 = 66$.

(iii) $72 \equiv -5 \pmod 7$ since 7 divides $72 - (-5) = 77$.

(iv) $27 \not\equiv 8 \pmod 9$ since 9 does not divide $27 - 8 = 19$.

Our first theorem (proved in Problem 11.40) states that congruence modulo m is an equivalence relation.

Theorem 11.20: Let m be a positive integer. Then:

(i) For any integer a, we have $a \equiv a \pmod m$.

(ii) If $a \equiv b \pmod m$, then $b \equiv a \pmod m$.

(iii) If $a \equiv b \pmod m$ and $b \equiv c \pmod m$, then $a \equiv c \pmod m$.

Remark: Suppose m is positive, and a is any integer. By the Division Algorithm, there exists integers q and r with $0 \leq r < m$ such that $a = mq + r$. Hence

$$mq = a - r \qquad \text{or} \qquad m|(a - r) \qquad \text{or} \qquad a \equiv r \pmod m$$

Accordingly:

(1) Any integer a is congruent modulo m to a unique integer in the set

$$\{0, 1, 2, \ldots, m - 1\}$$

The uniqueness comes from the fact that m cannot divide the difference of two such integers.

(2) Any two integers a and b are congruent modulo m if and only if they have the same remainder when divided by m.

Residue Classes

Since congruence modulo m is an equivalence relation, it partitions the set $\mathbf{Z}$ of integers into disjoint equivalence classes called the *residue classes modulo m*. By the above remarks, a residue class consists of all those integers with the same remainder when divided by m. Therefore, there are m such residue classes and each residue class contains exactly one of the integers in the set of possible remainders,

$$\{0, 1, \ldots, m-1\}$$

Generally speaking, a set of m integers $\{a_1, a_2, \ldots, a_m\}$ is said to be a *complete residue system modulo m* if each a_i comes from a distinct residue class. Thus the integers from 0 to $m-1$ form a complete residue system. In fact, any m consecutive integers form a complete residue system modulo m.

The notation $[x]_m$ or simply $[x]$ is used to denote the residue class (modulo m) containing an integer x, that is, those integers which are congruent to x. In other words,

$$[x] = \{a \in \mathbf{Z}: a \equiv x \pmod{m}\}.$$

Accordingly, the residue classes can be denoted by

$$[0], \quad [1], \quad [2], \quad \ldots, \quad [m-1]$$

or by using any other choice of integers in a complete residue system.

EXAMPLE 11.11 The residue classes modulo $m = 6$ follow:

$$[0] = \{\ldots, -18, -12, -6, 0, 6, 12, 18, \ldots\} \qquad [3] = \{\ldots, -15, -9, -3, 3, 9, 15, 21, \ldots\}$$
$$[1] = \{\ldots, -17, -11, -5, 1, 7, 13, 19, \ldots\} \qquad [4] = \{\ldots, -14, -8, -2, 4, 10, 16, 22, \ldots\}$$
$$[2] = \{\ldots, -16, -10, -4, 2, 8, 14, 20, \ldots\} \qquad [5] = \{\ldots, -13, -7, -1, 5, 11, 17, 23, \ldots\}$$

Note that $\{-2, -1, 0, 1, 2, 3\}$ is also a complete residue system modulo $m = 6$.

Congruence Arithmetic

The next theorem (proved in Problem 11.41) tells us that, under addition and multiplication, the congruence relation behaves very much like the relation of equality. Namely:

Theorem 11.21: Suppose $a \equiv c \pmod{m}$ and $b \equiv d \pmod{m}$. Then:
(i) $a + b \equiv c + d \pmod{m}$.
(ii) $a \cdot b \equiv c \cdot d \pmod{m}$.

Remark: Suppose $p(x)$ is a polynomial with integral coefficients. If $s \equiv t \pmod{m}$, then using Theorem 11.21 repeatedly we can show that $p(s) \equiv p(t) \pmod{m}$.

EXAMPLE 11.12 Observe that $2 \equiv 8 \pmod{6}$ and $5 \equiv 41 \pmod{6}$. Then:

(i) $2 + 5 \equiv 8 + 41 \pmod{6}$ or $7 \equiv 49 \pmod{6}$.

(ii) $2 \cdot 5 \equiv 8 \cdot 41 \pmod{6}$ or $10 \equiv 328 \pmod{6}$.

Suppose $p(x) = 3x^2 - 7x + 5$. Then

$$p(2) = 12 - 14 + 5 = 3 \qquad \text{and} \qquad p(8) = 192 - 56 + 5 = 141$$

Hence $3 \equiv 141 \pmod{6}$.

Arithmetic of Residue Classes

Addition and multiplication are defined for our residue classes modulo m as follows:

$$[a] + [b] = [a + b] \qquad \text{and} \qquad [a] \cdot [b] = [ab]$$

For example, consider the residue classes modulo $m = 6$; that is,

$$[0], \quad [1], \quad [2], \quad [3], \quad [4], \quad [5]$$

Then

$$[2] + [3] = [5], \quad [4] + [5] = [9] = [3], \quad [2] \cdot [2] = [4], \quad [2] \cdot [5] = [10] = [4]$$

The content of Theorem 11.21 tells us that the above definitions are well defined, that is, the sum and product of the residue classes do not depend on the choice of representative of the residue class.

There are only a finite number m of residue classes modulo m. Thus one can easily write down explicitly their addition and multiplication tables when m is small. Figure 11-4 shows the addition and multiplication tables for the residue classes modulo $m = 6$. For notational convenience, we have omitted brackets and simply denoted the residue classes by the numbers 0, 1, 2, 3, 4, 5.

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

×	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Fig. 11-4

Integers Modulo m, $\mathbf{Z}_m$

The *integers modulo m*, denoted by $\mathbf{Z}_m$, refers to the set

$$\mathbf{Z}_m = \{0, 1, 2, 3, \ldots, m-1\}$$

where addition and multiplication are defined by the arithmetic modulo m or, in other words, the corresponding operations for the residue classes. For example, Fig. 11-4 may also be viewed as the addition and multiplication tables for $\mathbf{Z}_6$. This means:

> There is no essential difference between $\mathbf{Z}_m$ and the arithmetic of the residue classes modulo m, and so they will be used interchangeably.

Cancelation Laws for Congruences

Recall that the integers satisfy the following:

> Cancelation law: if $ab = ac$ and $a \neq 0$, then $b = c$.

The critical difference between ordinary arithmetic and arithmetic modulo m is that the above cancelation law is false for congruences. For example,

$$3 \cdot 1 \equiv 3 \cdot 5 \pmod 6 \qquad \text{but} \qquad 1 \not\equiv 5 \pmod 6$$

That is, we cannot cancel the 3 even through $3 \not\equiv 0 \pmod 6$. However, we do have the following *Modified Cancelation Law* for our congruence relations.

Theorem 11.22 (Modified Cancelation Law): Suppose $ab \equiv ac \pmod m$ and $\gcd(a, m) = 1$. Then $b \equiv c \pmod m$.

The above theorem is a consequence of the following more general result (proved in Problem 11.44).

Theorem 11.23: Suppose $ab \equiv ac \pmod m$ and $d = \gcd(a, m)$. Then $b \equiv c \pmod{m/d}$.

EXAMPLE 11.13 Consider the following congruence:

$$6 \equiv 36 \pmod{10} \qquad (1)$$

Since 3 and the modulus 10 are relatively prime, we can divide both sides of (*1*) by 3, obtaining

$$2 \equiv 12 \pmod{10}$$

Observe that we cannot divide both sides of (*1*) by 6; that is,

$$1 \not\equiv 6 \pmod{10}$$

However, by Theorem 11.23, we can divide both sides of (*1*) by 6 if we also divide the modulus by $2 = \gcd(6, 10)$. That is,

$$1 \equiv 6 \pmod{5}.$$

Remark: Suppose p is a prime. Then the integers 1 through $p - 1$ are relatively prime to p. Thus the usual cancelation law does hold when the modulus is a prime p. That is:

> If $ab \equiv ac \pmod{p}$ and $a \not\equiv 0 \pmod{p}$, then $b \equiv c \pmod{p}$.

Thus $\mathbf{Z}_p$, the integers modulo a prime p, plays a very special role in number theory.

Reduced Residue Systems, Euler Phi Function

The modified cancelation law, Theorem 11.22, is indicative of the special role played by those integers which are relatively prime (coprime) to the modulus m. We note that a is coprime to m if and only if every element in the residue class $[a]$ is coprime to m. Thus we can speak of a residue class being coprime to m.

The number of residue classes relatively prime to m or, equivalently, the number of integers between 1 and m (inclusive) which are relatively prime to m is denoted by

$$\phi(\mathrm{m})$$

The function $\phi(m)$ is called the *Euler phi function*. The list of numbers between 1 and m which are coprime to m or, more generally, any list of $\phi(m)$ incongruent integers which are coprime to m, is called a *reduced residue system modulo m*.

EXAMPLE 11.14

(*a*) Consider the modulus $m = 15$. There are eight integers between 1 and 15 which are coprime to 15:

$$1, \quad 2, \quad 4, \quad 7, \quad 8, \quad 11, \quad 13, \quad 14$$

Thus $\phi(15) = 8$ and the above eight integers form a reduced residue system modulo 15.

(*b*) Consider any prime p. All the numbers $1, 2, \ldots, p - 1$ are coprime to p; hence $\phi(p) = p - 1$.

A function f with domain the positive integers $\mathbf{N}$ is said to be *multiplicative* if, whenever a and b are relatively prime,

$$f(ab) = f(a)\, f(b)$$

The following theorem (proved in Problem 11.51) applies.

Theorem 11.24: Euler's phi function is multiplicative. That is, if a and b are relatively prime, then

$$\phi(ab) = \phi(a)\phi(b).$$

11.9 CONGRUENCE EQUATIONS

A *polynomial congruence equation* or, simply, a *congruence equation* (in one unknown x) is an equation of the form

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 + a_0 \equiv 0 \pmod{m} \qquad (*)$$

Such an equation is said to be of *degree* n if $a_n \not\equiv 0 \pmod{m}$.

Suppose $s \equiv t \pmod{m}$. Then s is a solution of $(*)$ if and only if t is a solution of $(*)$. Thus the *number of solutions* of $(*)$ is defined to be the number of incongruent solutions or, equivalently, the number of solutions in the set

$$\{0, 1, 2, \ldots, m-1\}$$

Of course, these solutions can always be found by testing, that is, by substituting each of the m numbers into $(*)$ to see if it does indeed satisfy the equation.

The *complete set of solutions* of $(*)$ is a maximum set of incongruent solutions whereas the *general solution* of $(*)$ is the set of all integral solutions of $(*)$. The general solution of $(*)$ can be found by adding all the multiples of the modulus m to any complete set of solutions.

EXAMPLE 11.15 Consider the equations:

(*a*) $x^2 + x + 1 \equiv 0 \pmod{4}$

(*b*) $x^2 + 3 \equiv 0 \pmod{6}$.

(*c*) $x^2 - 1 \equiv 0 \pmod{8}$.

Here we find the solutions by testing.

(*a*) There are no solutions since 0, 1, 2, and 3 do not satisfy the equation.

(*b*) There is only one solution among $0, 1, \ldots, 5$ which is 3. Thus the general solution consists of the integers $3 + 6k$ where $k \in \mathbf{Z}$.

(*c*) There are four solutions, 1, 3, 5 and 7. This shows that a congruence equation of degree n can have more than n solutions.

We emphasize that we are not only interested in studying congruence equations in order to find their solutions; this can always be found by testing. We are mainly interested in developing techniques to help us find such solutions, and a theory which tells us conditions under which solutions exist and the number of such solutions. Such a theory holds for linear congruence equations which we investigate below. We will also discuss the Chinese Remainder Theorem, which is essentially a system of linear congruences.

Remark 1: The coefficients of a congruence equation can always be reduced modulo m since an *equivalent equation*, that is, an equation with the same solutions, would result. For example,

$$15x^2 + 28x + 14 \equiv 0 \pmod{6}, \qquad 3x^2 + 4x + 2 \equiv 0 \pmod{6}, \qquad 3x^2 - 2x + 2 \equiv 0 \pmod{6},$$

are equivalent equations since the coefficients are congruent modulo $m = 6$. Usually we choose coefficients between 0 and $m - 1$ or between $-m/2$ and $m/2$.

Remark 2: Since we are really looking for solutions of $(*)$ among the residue classes modulo m rather than among the integers, we may view $(*)$ as an equation over $\mathbf{Z}_m$, the integers modulo m, rather than an equation over $\mathbf{Z}$, the integers. In this context, the number of solutions of $(*)$ is simply the number of solutions in $\mathbf{Z}_m$.

Linear Congruence Equation: $ax \equiv 1 \pmod{m}$

First we consider the special linear congruence equation

$$ax \equiv 1 \pmod{m} \qquad (**)$$

where $a \not\equiv 0 \pmod{m}$. The complete story of this equation is given in the following theorem (proved in Problem 11.65).

Theorem 11.25: If a and m are relatively prime, then $ax \equiv 1 \pmod{m}$ has a unique solution; otherwise it has no solution.

EXAMPLE 11.16

(*a*) Consider the congruence equation

$$6x \equiv 1 \pmod{33}$$

Observe that $\gcd(6, 33) = 3$. Thus the equation has no solution.

(*b*) Consider the congruence equation

$$7x \equiv 1 \pmod{9}$$

Here $\gcd(7, 9) = 1$; hence the equation has a unique solution. Testing the numbers $0, 1, \ldots, 8$, we find that

$$7(4) = 28 \equiv 1 \pmod{9}$$

Thus $x = 4$ is our unique solution. (The general solution is $4 + 9k$ for $k \in \mathbf{Z}$.)

Suppose a solution of $(**)$ does exist, that is, suppose $\gcd(a, m) = 1$, and suppose the modulus m is large. Then the Euclidean algorithm can be used to find a solution of $(**)$. Specifically, we use the Euclidean algorithm to find x_0 and y_0 such that

$$ax_0 + my_0 = 1$$

From this it follows that $ax_0 \equiv 1 \pmod{m}$; that is, x_0 is a solution to $(**)$.

EXAMPLE 11.17

Consider the following congruence equation:

$$81x \equiv 1 \pmod{256}$$

By observation or by applying the Euclidean algorithm to 81 and 256, we find that $\gcd(81, 256) = 1$. Thus the equation has a unique solution. Testing may not be an efficient way to find this solution since the modulus $m = 256$ is relatively large. Hence, we apply the Euclidean algorithm to $a = 81$ and $m = 256$. That is, as in Example 11.6, we find $x_0 = -25$ and $y_0 = 7$ such that

$$81x_0 + 256y_0 = 1$$

This means that $x_0 = -25$ is a solution of the given congruence equation. Adding $m = 256$ to -25, we obtain the unique solution

$$x = 231$$

between 0 and 256.

Linear Congruence Equation: $ax \equiv b \pmod{m}$

Now we consider the more general linear congruence equation

$$ax \equiv b \pmod{m} \qquad (***)$$

where $a \not\equiv 0 \pmod{m}$. We first consider the case (proved in Problem 11.66) where a and m are coprime.

Theorem 11.26: Suppose a and m are relatively prime. Then $ax \equiv b \pmod{m}$ has a unique solution. Moreover, if s is the unique solution to $ax \equiv 1 \pmod{m}$, then

$$x = bs$$

is the unique solution to $ax \equiv b \pmod{m}$.

EXAMPLE 11.18

(*a*) Consider the congruence equation

$$3x \equiv 5 \pmod{8}$$

Since 3 and 8 are coprime, the equation has a unique solution. Testing the integers $0, 1, \ldots, 7$, we find that

$$3(7) = 21 \equiv 5 \pmod{8}$$

Thus $x = 7$ is the unique solution of the equation.

(*b*) Consider the congruence equation

$$33x \equiv 38 \pmod{280} \tag{1}$$

Since $\gcd(33, 280) = 1$, the equation has a unique solution. Testing may not be an efficient way to find this solution since the modulus $m = 280$ is relatively large. We apply the Euclidean algorithm to first find a solution to

$$33x \equiv 1 \pmod{280} \tag{2}$$

That is, as in Example 11.6, we find $x_0 = 17$ and $y_0 = -2$ to be a solution of

$$33x_0 + 280y_0 = 1$$

This means that $s = 17$ is a solution of equation (*2*). Then

$$sb = 17(38) = 646$$

is a solution of the original equation (*1*). Dividing 646 by $m = 280$, we obtain the remainder

$$x = 86$$

which is the unique solution (*1*) between 0 and 280. (The general solution is $86 + 280k$ with $k \in \mathbf{Z}$.)

The complete story of the general case of $(***)$ is contained in the following theorem (proved in Problem 11.67).

Theorem 11.27: Consider the equation $ax \equiv b \pmod{m}$ where $d = \gcd(a, m)$.

(i) Suppose d does not divide b. Then $ax \equiv b \pmod{m}$ has no solution.

(ii) Suppose d does divide b. Then $ax \equiv b \pmod{m}$ has d solutions which are all congruent modulo M to the unique solution of

$$Ax \equiv B \pmod{M}$$

where $A = a/d$, $B = b/d$, and $M = m/d$.

Observe that Theorem 11.26 applies to the equation $Ax \equiv B \pmod{M}$ in Theorem 11.27 since $\gcd(A, M) = 1$.

EXAMPLE 11.19 Solve each congruence equation: (*a*) $4x \equiv 9 \pmod{14}$, (*b*) $8x \equiv 12 \pmod{28}$.

(*a*) Note $\gcd(4, 14) = 2$. However, 2 does not divide 9. Hence the equation does not have a solution.

(*b*) Note that $d = \gcd(8, 28) = 4$, and $d = 4$ does divide 12. Thus the equation has $d = 4$ solutions. Dividing each term in the equation by $d = 4$ we obtain the congruence equation

$$2x \equiv 3 \pmod{7} \tag{1}$$

which has a unique solution. Testing the integers $0, 1, \ldots, 6$, we find that 5 is the unique solution of (*1*). We now add up to $d - 1 = 3$ multiples of 7 to the solution 5 of (*1*) obtaining:

$$5 + 7 = 12, \qquad 5 + 2(7) = 19, \qquad 5 + 3(7) = 26$$

Accordingly, 5, 12, 19, 26 are the required $d = 4$ solutions of the original equation (*b*).

Remark: The solution of equation (*1*) in Example 11.19 was obtained by inspection. However, in case the modulus m is large, we can always use the Euclidean algorithm to find its unique solution as in Example 11.17. (See Problem 11.61.)

Chinese Remainder Theorem

An old Chinese riddle asks the following question.

> Is there a positive integer x such that when x is divided by 3 it yields a remainder 2, when x is divided by 5 it yields a remainder 4, and when x is divided by 7 it yields a remainder 6?

In other words, we seek a common solution of the following three congruence equations:

$$x \equiv 2 \pmod{3}, \qquad x \equiv 4 \pmod{5}, \qquad x \equiv 6 \pmod{7}$$

Observe that the moduli 3, 5 and 7 are pairwise relatively prime. (Moduli is the plural of modulus.) Thus the following theorem applies; it tells us that there is a unique solution modulo $M = 3 \cdot 5 \cdot 7 = 105$.

Theorem 11.28 (Chinese Remainder Theorem): Given the system

$$x \equiv r_1 \pmod{m_1}, \qquad x \equiv r_2 \pmod{m_2}, \qquad \ldots, \qquad x \equiv r_k \pmod{m_k} \tag{$*$}$$

where the m_i are pairwise relatively prime. Then the system has a unique solution modulo $M = m_1 m_2 \cdots m_k$.

One can actually give an explicit formula for the solution of the system $(*)$ in Theorem 11.28 which we state as a proposition.

Proposition 11.29: Consider the system $(*)$ of congruence equations. Let $M = m_1 m_2 \cdots m_k$ and

$$M_1 = \frac{M}{m_1}, \qquad M_2 = \frac{M}{m_2}, \qquad \ldots, \qquad M_k = \frac{M}{m_k}$$

(Then each pair M_i and m_i are co-prime.) Let $s_1, s_2, \ldots, s_k$ be the solutions, respectively, of the congruence equations

$$M_1 x \equiv 1 \pmod{m_1}, \quad M_2 x \equiv 1 \pmod{m_2}, \quad \cdots \quad M_k x \equiv 1 \pmod{m_k}$$

Then

$$X_0 = M_1 s_1 r_1 + M_2 s_2 r_2 + \cdots + M_k s_k r_k \tag{$**$}$$

is a solution of the system $(*)$.

We now solve the original riddle in two ways.

Method 1: First we apply the theorem to the first two equations,

$$(a) \quad x \equiv 2 \pmod 3 \qquad \text{and} \qquad (b) \quad x \equiv 4 \pmod 5$$

The theorem tells us there is a unique solution modulo $M = 3 \cdot 5 = 15$. Adding multiples of the modulus $m = 5$ to the given solution $x = 4$ of the second equation (b), we obtain the following three solutions of (b) which are less than 15:

$$4, \quad 9, \quad 14$$

Testing each of these solutions in equation (a), we find that 14 is the only solution of both equations.

Now we apply the same process to the two equations

$$(c) \quad x \equiv 14 \pmod{15} \qquad \text{and} \qquad (d) \quad x \equiv 6 \pmod 7$$

The theorem tells us there is a unique solution modulo $M = 15 \cdot 7 = 105$. Adding multiples of the modulus $m = 15$ to the given solution $x = 14$ of the first equation (c), we obtain the following seven solutions of (b) which are less than 105:

$$14, \quad 29, \quad 44, \quad 59, \quad 74, \quad 89, \quad 104$$

Testing each of these solutions of (c) in the second equation (d), we find that 104 is the only solution of both equations. Thus

$$x = 104$$

is the smallest positive integer satisfying all three equations, that is, which is a solution of the riddle.

Method 2: Using the above notation, we obtain

$$M = 3 \cdot 5 \cdot 7 = 105, \qquad M_1 = 105/3 = 35, \qquad M_2 = 105/5 = 21, \qquad M_3 = 105/7 = 15$$

We now seek solutions to the equations

$$35x \equiv 1 \pmod 3, \qquad 21x \equiv 1 \pmod 5, \qquad 15x \equiv 1 \pmod 7$$

Reducing 35 modulo 3, reducing 21 modulo 5, and reducing 15 modulo 7, we obtain the system

$$2x \equiv 1 \pmod 3, \qquad x \equiv 1 \pmod 5, \qquad x \equiv 1 \pmod 7$$

The solutions of these three equations are, respectively,

$$s_1 = 2, \qquad s_2 = 1, \qquad s_3 = 1$$

We now substitute into the formula $(**)$ to obtain the following solution of our original system:

$$x_0 = 35 \cdot 2 \cdot 2 + 21 \cdot 1 \cdot 4 + 15 \cdot 1 \cdot 6 = 314$$

Dividing this solution by the modulus $M = 105$, we obtain the remainder

$$x = 104$$

which is the unique solution of the riddle between 0 and 105.

Remark: The above solutions $s_1 = 2$, $s_2 = 1$, $s_3 = 1$ were obtained by inspection. If the moduli are large, we can always use the Euclidean algorithm to find such solutions as in Example 11.17.

© The McGraw–Hill Companies, 2004

Solved Problems

INEQUALITIES, ABSOLUTE VALUE

11.1. Insert the correct symbol, $<$, $>$, or $=$, between each pair of integers:

(a) $4 \_\_\_\_ -7$, (c) $3^2 \_\_\_\_ 5$, (e) $3^2 \_\_\_\_ 9$

(b) $-2 \_\_\_\_ -9$, (d) $-8 \_\_\_\_ 3$, (f) $6 \_\_\_\_ 8$

For each pair of integers, say a and b, determine their relative positions on the number line $\mathbf{R}$; or, alternatively, compute $b - a$, and write

$$a < b, \qquad a > b, \qquad \text{or} \qquad a = b$$

according as $b - a$ is positive, negative, or zero. Hence:

(a) $4 > -7$; (b) $-2 > -9$; (c) $3^2 > 5$; (d) $-8 < 3$; (e) $3^2 = 9$, $6 < 8$.

11.2. Evaluate: (a) $|-4|$, $|3|$, $|0|$; (b) $|2-5|$, $|-2+5|$, $|-2-5|$; (c) $|5-8|+|2-4|$, $|4-3|-|3-9|$.

(a) The absolute value is the magnitude of the number without regard to sign. Hence:

$$|-4| = 4, \qquad |3| = 3, \qquad |0| = 0$$

(b) Evaluate inside the absolute value sign first:

$$|2-5| = |-3| = 3, \qquad |-2+5| = |3| = 3, \qquad |-2-5| = |-7| = 7$$

(c) Evaluate inside the absolute value sign first:

$$|5-8| + |2-4| = |-3| + |-2| = 3 + 2 = 5$$

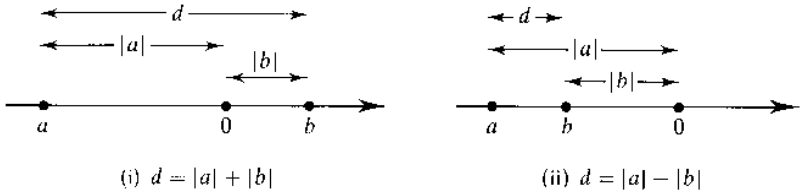
$$|4-3| - |3-9| = |1| - |-6| = 1 - 6 = -5$$

11.3. Find the distance d between each pair of integers:

(a) 3 and -7; (b) -4 and 2; (c) 1 and 9; (d) -8 and -3; (e) 4 and -4; (f) -5 and -8.

The distance d between a and b is given by $d = |a-b| = |b-a|$. Alternatively, as indicated by Fig. 11-5, $d = |a| + |b|$ when a and b have different signs, and $d = |a| - |b|$ when a and b have the same sign and $|a| \geq |b|$.

Thus: (a) $d = 3 + 7 = 10$; (b) $d = 4 + 2 = 6$; (c) $d = 9 - 1 = 8$; (d) $d = 8 - 3 = 5$; (e) $d = 4 + 4 = 8$; (f) $d = 8 - 5 = 3$.



(i) $d = |a| + |b|$ (ii) $d = |a| - |b|$

Fig. 11-5

11.4. Find all integers n such that: (a) $1 < 2n - 6 < 14$; (b) $2 < 8 - 3n < 18$.

(a) Add 6 to the "three sides" to get $7 < 2n < 20$. Then divide all sides by 2 (or multiply by $\frac{1}{2}$) to get $3.5 < n < 10$. Hence

$$n = 4, 5, 6, 7, 8, 9$$

(*b*) Add -8 to the three sides to get $-6 < -3n < 10$. Divide by -3 (or multiply by $-\frac{1}{3}$) and, since -3 is negative, change the direction of the inequality to get

$$2 > n > -3.3 \qquad \text{or} \qquad -3.3 < n < 2$$

Hence $n = -3, -2, -1, 0, 1$.

11.5. Prove Proposition 11.1 (iii): If $a \leq b$ and $b \leq c$, then $a \leq c$.

The proposition is clearly true when $a = b$ and $b = c$. Thus we need only consider the case that $a < b$ and $b < c$. Hence $b - a$ and $c - b$ are positive. Therefore, by property $[\mathbf{P}_1]$ of the positive integers $\mathbf{N}$, the sum is also positive. That is,

$$(b - a) + (c - b) = c - a$$

is positive. Thus $a < c$ and hence $a \leq c$.

11.6. Prove Proposition 11.3: Suppose $a \leq b$, and c is any integer. Then:
(i) $a + c \leq b + c$, (ii) $ac \leq bc$ when $c > 0$; but $ac \geq bc$ when $c < 0$.

The proposition is certainly true when $a = b$. Hence we need only consider the case when $a < b$, that is, when $b - a$ is positive.

(i) The following difference is positive:

$$(b + c) - (a + c) = b - a$$

Hence $a + c < b + c$.

(ii) Suppose c is positive. By property $[\mathbf{P}_1]$ of the positive integers $\mathbf{N}$, the following product is also positive:

$$c(b - a) = bc - ac$$

Thus $ac < bc$. Now suppose c is negative. Then $-c$ is positive, and the following product is also positive:

$$(-c)(b - a) = ac - bc$$

Accordingly, $bc < ac$, whence $ac > bc$.

11.7. Prove Proposition 11.4 (iii): $|ab| = |a|\ |b|$.

The proof consists of a case by case analysis.

(*a*) Suppose $a = 0$ or $b = 0$.

Then $|a| = 0$ or $|b| = 0$, and so $|a|\ |b| = 0$. Also $ab = 0$. Hence

$$|ab| = 0 = |a|\ |b|$$

(*b*) Suppose $a > 0$ and $b > 0$.

Then $|a| = a$ and $|b| = b$. Hence

$$|ab| = ab = |a|\ |b|$$

.

(*c*) Suppose $a > 0$ and $b < 0$.

Then $|a| = a$ and $|b| = -b$. Also $ab < 0$. Hence

$$|ab| = -(ab) = a(-b) = |a|\ |b|$$

(*d*) Suppose $a < 0$ and $b > 0$.

Then $|a| = -a$ and $|b| = b$. Also $ab < 0$. Hence

$$|ab| = -(ab) = (-a)b = |a|\ |b|$$

(*e*) Suppose $a < 0$ and $b < 0$.

Then $|a| = -a$ and $|b| = -b$. Also $ab > 0$. Hence

$$|ab| = ab = (-a)(-b) = |a|\ |b|$$

11.8. Prove Proposition 11.4 (iv): $|a \pm b| \leq |a| + |b|$.

Now $ab \leq |ab| = |a|\ |b|$, and so $2ab \leq 2|a|\ |b|$. Hence

$$(a+b)^2 = a^2 + 2ab + b^2 \leq |a|^2 + 2|a|\ |b| + |b|^2 = (|a| + |b|)^2$$

But $\sqrt{(a+b)^2} = |a+b|$. Thus the square root of the above yields $|a+b| \leq |a| + |b|$. Also,

$$|a-b| = |a + (-b)| \leq |a| + |-b| = |a| + |b|$$

MATHEMATICAL INDUCTION, WELL-ORDERING PRINCIPLE

11.9. Prove the proposition that the sum of the first n positive integers is $n(n+1)/2$; that is

$$P(n): \quad 1 + 2 + \cdots + n = \tfrac{1}{2}n(n+1)$$

The proposition holds for $n = 1$ since

$$P(1): \quad 1 = \tfrac{1}{2}(1)(1+1)$$

Assuming $P(n)$ is true, we add $n+1$ to both sides of $P(n)$ obtaining

$$\begin{aligned} 1 + 2 + 3 + \cdots + n + (n+1) &= \tfrac{1}{2}n(n+1) + (n+1) \\ &= \tfrac{1}{2}[n(n+1) + 2(n+1)] \\ &= \tfrac{1}{2}[(n+1)(n+2)] \end{aligned}$$

which is $P(n+1)$. That is, $P(n+1)$ is true whenever $P(n)$ is true. By the principle of induction, P is true for every $n \in \mathbf{N}$.

11.10. Prove the proposition P that the sum of the squares of the first n positive integers is $n(n+1)(2n+1)/6$; that is

$$P(n): \quad 1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

$P(1)$ is true since

$$1^2 = \frac{1(1+1)(2 \cdot 1 + 1)}{6}$$

Assuming $P(n)$ is true, we add $(n+1)^2$ to both sides of $P(n)$, obtaining

$$\begin{aligned}1^2 + 2^2 + \cdots + n^2 + (n+1)^2 &= \frac{n(n+1)(2n+1)}{6} + (n+1)^2 \\ &= \frac{n(n+1)(2n+1) + 6(n+1)^2}{6} \\ &= \frac{(n+1)[n(2n+1) + 6(n+1)]}{6} \\ &= \frac{(n+1)(2n^2 + 7n + 6)}{6} \\ &= \frac{(n+1)(n+2)(2n+3)}{6} \\ &= \frac{(n+1)[(n+1)+1][2(n+1)+1]}{6}\end{aligned}$$

which is $P(n+1)$. Thus $P(n+1)$ is true whenever $P(n)$ is true. By the principle of induction, P is true for all $n \in \mathbf{N}$.

11.11. Suppose $a \neq 1$. Let P be the proposition on $n \geq 1$ defined by

$$P(n): \quad 1 + a + a^2 + \cdots + a^n = \frac{a^{n+1} - 1}{a - 1}$$

Show P is true for all n.

$P(1)$ is true since

$$1 + a = \frac{a^2 - 1}{a - 1}$$

Assuming $P(n)$ is true, we add a^{n+1} to both sides of $P(n)$, obtaining

$$\begin{aligned}1 + a + a^2 + \cdots + a^n + a^{n+1} &= \frac{a^{n+1} - 1}{a - 1} + a^{n+1} \\ &\quad \frac{a^{n+1} - 1 + (a-1)a^{n+1}}{a - 1} \\ &= \frac{a^{n+2} - 1}{a - 1}\end{aligned}$$

which is $P(n+1)$. Thus $P(n+1)$ is true whenever $P(n)$ is true. By the principle of induction, P is true for all $n \in \mathbf{N}$.

11.12. Prove: If $n \in \mathbf{Z}$ and n is a positive integer, then $n \geq 1$. (This is not true for the rational numbers $\mathbf{Q}$.) In other words, if $P(n)$ is the statement that $n \geq 1$, then $P(n)$ is true for every $n \in \mathbf{N}$.

Method 1: (Mathematical Induction)

$P(n)$ holds for $n = 1$ since $1 \geq 1$. Assuming $P(n)$ is true, that is, $n \geq 1$, add 1 to both sides to obtain

$$n + 1 \geq 2 > 1$$

which is $P(n+1)$. That is, $P(n+1)$ is true whenever $P(n)$ is true. By the principle of mathematical induction, P is true for every $n \in \mathbf{N}$.

Method 2: (Well-ordering Principle)

Suppose there does exist a positive integer less than 1. By the well-ordering principle, there exists a least positive integer a such that

$$0 < a < 1$$

Multiplying the inequality by the positive integer a we obtain

$$0 < a^2 < a$$

Therefore, a^2 is a positive integer less than a which is also less than 1. This contradicts a's property of being the least positive integer less than 1. Thus there exists no positive integer less than 1.

11.13. Suppose a and b are positive integers. Prove: (a) If $b \neq 1$, then $a < ab$. (b) If $ab = 1$, then $a = 1$ and $b = 1$. (c) If n is composite, then $n = ab$ where $1 < a, b < n$.

(a) By Problem 11.12, $b > 1$. Hence $b - 1 > 0$, that is, $b - 1$ is positive. By the property $[\mathbf{P}_1]$ of the positive integers $\mathbf{N}$, the following product is also positive:

$$a(b - 1) = ab - a$$

Thus $a < ab$, as required.

(b) Suppose $b \neq 1$. By (a), $a < ab = 1$. This contradicts Problem 11.12; hence $b = 1$. It then follows that $a = 1$.

(c) If n is not prime, then n has a positive divisor a such that $a \neq 1$ and $a \neq n$. Then $n = ab$ where $b \neq 1$ and $b \neq n$. Thus, by Problem 11.12 and by part (a), $1 < a, b < ab = n$.

11.14. Prove Theorem 11.6 (Well-ordering Principle): Let S be a nonempty set of positive integers. Then S contains a least element.

Suppose A has no least element. Let M consist of those positive integers which are less than every element of S. Then $1 \in M$; otherwise, $1 \in S$ and 1 would be a least element of S. Suppose $k \in M$. Then k is less than every element of S. Therefore $k + 1 \in M$; otherwise $k + 1$ would be a least element of S.

By the principle of mathematical induction M contains every positive integer. Thus S is empty. This contradicts the hypothesis that S is nonempty. Accordingly, the original assumption that S has no least element cannot be true. Thus the theorem is true.

11.15. Prove Theorem 11.5 (Induction: Second Form): Let P be a proposition defined on the integers $n \geq 1$ such that:

(i) $P(1)$ is true.

(ii) $P(n)$ is true whenever $P(k)$ is true for all $1 \leq k < n$. Then P is true for all $n \geq 1$

Let A be the set of integers $n \geq 1$ for which P is not true. Suppose A is not empty. By the well-ordering principle, A contains at least element a_0. By (i), $a_0 \neq 1$.

Since a_0 is the least element of A, P is true for every integer k where $1 \leq k < a_0$. By (ii), P is true for a_0. This contradicts the fact that $a_0 \in A$. Hence A is empty, and so P is true for every integer $n \geq 1$.

DIVISION ALGORITHM

11.16. For each pair of integers a and b, find integers q and r such that $a = bq + r$ and $0 \leq r < |b|$:

(a) $a = 258$ and $b = 12$; (b) $a = 573$ and $b = -16$.

(a) Here a and b are positive. Simply divide a by b, that is, 258 by 12, say, as in Fig. 11-6(a). Then $q = 21$ and $r = 6$.

(b) Here a is positive, but b is negative. Divide a by $|b|$, that is, 573 by 16, say, as in Fig. 11-6(b). Then

$$573 = (16)(35) + 13 = 573 = (-16)(-35) + 13$$

Thus $q = -35$ and $r = 13$.

$$\begin{array}{r} 21 \\ 12\overline{)258} \\ \underline{24} \\ 18 \\ \underline{12} \\ 6 \end{array} \qquad \begin{array}{r} 35 \\ 16\overline{)573} \\ \underline{48} \\ 93 \\ \underline{80} \\ 13 \end{array} \qquad \begin{array}{r} 27 \\ 14\overline{)381} \\ \underline{28} \\ 101 \\ \underline{98} \\ 3 \end{array} \qquad \begin{array}{r} 25 \\ 17\overline{)433} \\ \underline{34} \\ 93 \\ \underline{85} \\ 8 \end{array}$$

(a) (b) (c) (d)

Fig. 11-6

11.17. For each pair of integers a and b, find integers q and r such that $a = bq + r$ and $0 \leq r < |b|$:

(a) $a = -381$ and $b = 14$; (b) $a = -433$ and $b = -17$.

Here a is negative in each case, hence we have to make some adjustments to be sure that $0 \leq r < |b|$.

(a) Divide $|a| = 381$ by $b = 14$, say, as in Fig. 11-6(c). Then

$$381 = (14)(27) + 3 \qquad \text{and so} \qquad -381 = (14)(-27) - 3$$

But -3 is negative and cannot be the remainder r; hence we add and subtract $b = 14$ as follows:

$$-381 = (14)(-27) - 14 + 14 - 3 = (14)(-28) + 11$$

Thus $q = -28$ and $r = 11$.

(b) Divide $|a| = 433$ by $|b| = 17$, say, as in Fig. 11-6(d). Then

$$433 = (17)(25) + 8 \qquad \text{and so} \qquad -433 = (-17)(25) - 8$$

But -8 is negative and cannot be the remainder r; we correct this by adding and subtracting $|b| = 17$ as follows:

$$-433 = (-17)(25) - 17 + 17 - 8 = (-17)(26) + 9$$

Thus $q = 26$ and $r = 9$.

11.18. Prove each of the following statements:

(a) Any integer a is of the form $3k$, $3k + 1$, or $3k + 2$.

(b) One of three consecutive integers is a multiple of 3.

(a) By the division algorithm

$$a = 3q + r \qquad \text{with} \qquad 0 \leq r < 3$$

From the last inequality, $r = 0$, 1, or 2. Hence

$$a = 3q, \qquad a = 3q + 1, \qquad \text{or} \qquad a = 3q + 2$$

(b) Let the three consecutive integers be a, $a + 1$, and $a + 2$. By part (a), $a = 3k$ or $a = 3k + 1$ or $a = 3k + 2$. If $a = 3k$, then a is a multiple of 3. If $a = 3k + 1$, then

$$a + 2 = 3k + 1 + 2 = 3(k + 1)$$

Hence $a + 2$ is a multiple of 3. If $a = 3k + 2$, then

$$a + 1 = 3k + 2 + 1 = 3(k + 1)$$

Hence $a + 1$ is a multiple of 3.

11.19. Prove $\sqrt{2}$ is not rational, that is, $\sqrt{2} \neq a/b$ where a and b are integers.

Suppose $\sqrt{2}$ is rational and $\sqrt{2} = a/b$ where a and b are integers reduced to lowest terms, i.e., $\gcd(a, b) = 1$. Squaring both sides yields

$$2 = \frac{a^2}{b^2} \qquad \text{or} \qquad a^2 = 2b^2$$

Then 2 divides a^2. Since 2 is a prime, $2|a$. Say $a = 2c$. Then

$$2b^2 = a^2 = 4c^2 \qquad \text{or} \qquad b^2 = 2c^2$$

Then 2 divides b^2. Since 2 is a prime $2|b$. Thus 2 divides both a and b. This contradicts the assumption that $\gcd(a, b) = 1$. Therefore, $\sqrt{2}$ is not rational.

11.20. Prove Theorem 11.7 (Division Algorithm) for the case of positive integers. That is, assuming a and b are positive integers, prove there exist nonnegative integers q and r such that

$$a = bq + r \qquad \text{and} \qquad 0 \leq r < b \tag{$*$}$$

If $a < b$, choose $q = 0$ and $r = a$. If $a = b$, choose $q = 1$ and $r = 0$. In either case, q and r satisfy $(*)$.

The proof is now by induction on a. If $a = 1$ then $a < b$ or $a = b$; hence the theorem holds when $a = 1$. Suppose $a > b$. Then $a - b$ is positive and $a - b < a$. By induction, the theorem holds for $a - b$. Thus there exists q' and r' such that

$$a - b = bq' + r' \qquad \text{and} \qquad 0 \leq r' < b$$

Then

$$a = bq' + b + r' = b(q' + 1) + r'$$

Choose $q = q' + 1$ and $r = r'$. Then q and r are nonnegative integers and satisfy $(*)$.

11.21. Prove Theorem 11.7 (Division Algorithm): Let a and b be integers with $b \neq 0$. Then there exists integers q and r such that

$$a = bq + r \qquad \text{and} \qquad 0 \leq r < |b|$$

Also, the integers q and r are unique.

Let M be the set of nonnegative integers of the form $a - xb$ for some integer x. If $x = -|a|b$, then $a - xb$ is nonnegative (Problem 11.78); hence M is nonempty. By the well-ordering principle, M has a least element, say r. Since $r \in M$, we have

$$r \geq 0 \qquad \text{and} \qquad r = a - qb$$

for some integer q. We need only show that $r < |b|$. Suppose $r \geq |b|$. Let $r' = r - |b|$. Then $r' \geq 0$ and also $r' < r$ because $b \neq 0$. Furthermore,

$$r' = r - |b| = a - qb - |b| = \begin{cases} a - (q+1)b, & \text{if } b < 0 \\ a - (q-1)b, & \text{if } b > 0 \end{cases}$$

In either case, r' belongs to M. This contradicts the fact that r is the least element of M. Accordingly, $r < |b|$. Thus the existence of q and r is proved.

We now show that q and r are unique. Suppose there exist integers q and r and q' and r' such that

$$a = bq + r \qquad \text{and} \qquad a = bq' + r' \qquad \text{and} \qquad 0 \leq r, r' < |b|$$

Then $bq + r = bq' + r'$; hence

$$b(q - q') = r' - r$$

Thus b divides $r' - r$. But $|r' - r| < |b|$ since $0 \leq r, r' < |b|$. Accordingly, $r' - r = 0$. This implies $q - q' = 0$ since $b \neq 0$. Consequently, $r' = r$ and $q' = q$; that is, q and r are uniquely determined by a and b.

DIVISIBILITY, PRIMES, GREATEST COMMON DIVISOR

11.22. Find all positive divisors of: (*a*) 18; (*b*) $256 = 2^8$; (*c*) $392 = 2^3 \cdot 7^2$.

(*a*) Since 18 is relatively small, we simply write down all positive integers (≤ 18) which divide 18. These are:

$$1, \quad 2, \quad 3, \quad 6, \quad 9, \quad 18$$

(*b*) Since 2 is a prime, the positive divisors of $256 = 2^8$ are simply the lower powers of 2, i.e.,

$$2^0, \quad 2^1, \quad 2^2, \quad 2^3, \quad 2^4, \quad 2^5, \quad 2^6, \quad 2^7, \quad 2^8$$

In other words, the positive divisors of 256 are:

$$1, \quad 2, \quad 4, \quad 8, \quad 16, \quad 32, \quad 64, \quad 128, \quad 256$$

(*c*) Since 2 and 7 are prime, the positive divisors of $392 = 2^3 \cdot 7^2$ are products of lower powers of 2 times lower powers of 7, i.e.,

$$2^0 \cdot 7^0, \quad 2^1 \cdot 7^0, \quad 2^2 \cdot 7^0, \quad 2^3 \cdot 7^0, \quad 2^0 \cdot 7^1, \quad 2^1 \cdot 7^1, \quad 2^2 \cdot 7^1, \quad 2^3 \cdot 7^1,$$
$$2^0 \cdot 7^2, \quad 2^1 \cdot 7^2, \quad 2^2 \cdot 7^2, \quad 2^3 \cdot 7^2$$

In other words, the positive powers of 392 are:

$$1, \quad 2, \quad 4, \quad 8, \quad 7, \quad 14, \quad 28, \quad 56, \quad 49, \quad 98, \quad 196, \quad 392.$$

(We have used the usual convention that $n^0 = 1$ for any nonzero number n.)

11.23. List all primes between 50 and 100.

Simply list all numbers p between 50 and 100 which cannot be written as a product of two positive integers, excluding 1 and p. This yields:

$$51, \quad 53, \quad 57, \quad 59, \quad 61, \quad 67, \quad 71, \quad 73, \quad 79, \quad 83, \quad 87, \quad 89, \quad 91, \quad 93, \quad 97$$

11.24. Let $a = 8316$ and $b = 10\,920$.

(*a*) Find $d = \gcd(a, b)$, the greatest common divisor of a and b.

(*b*) Find integers m and n such that $d = ma + nb$.

(*c*) Find $\text{lcm}(a, b)$, the least common multiple of a and b.

(*a*) Divide the smaller number $a = 8316$ into the large numer $b = 10\,920$, and then repeatedly divide each remainder into the divisor until obtaining a zero remainder. These steps are pictured in Fig. 11-7. The last nonzero remainder is 84. Thus

$$84 = \gcd(8316, \ 10\,920)$$

$$\begin{array}{r} 1 \\ 8316\overline{)10920} \\ \uparrow\ \underline{8316} \\ \quad 2604 \end{array} \qquad \begin{array}{r} 3 \\ 2604\overline{)8316} \\ \uparrow\ \underline{7812} \\ \quad 504 \end{array} \qquad \begin{array}{r} 5 \\ 504\overline{)2604} \\ \uparrow\ \underline{2520} \\ \quad 84 \end{array} \qquad \begin{array}{r} 6 \\ 84\overline{)504} \\ \underline{504} \\ 0 \end{array}$$

Fig. 11-7

(*b*) Now we find m and n such that

$$84 = 8316m + 1092n$$

The first three quotients in Fig. 11-7 yields the equations:

(*1*) $10\,920 = 1(8316) + 2604$; or $2604 = 10\,920 - 1(8316)$

(*2*) $8316 = 3(2604) + 504$; or $504 = 8316 - 3(2604)$

(*3*) $2604 = 5(504) + 84$; or $84 = 2604 - 5(504)$

Equation (*3*) tells us that 84 is a linear combination of 2604 and 504. We use (*2*) to replace 5044 in (*3*) so we can write 84 as a linear combination of 2604 and 8316 as follows:

(*4*) $84 = 2604 - 5(8316 - 3(2604)) = 2604 - 5(8316) + 15(2604)$
$= 16(2604) - 5(8316)$

We now use (*1*) to replace 2604 in (*4*) so we can write 84 as a linear combination of 8316 and 10 920 as follows:

$$\begin{aligned} 84 &= 16(10\,920 - 1(8316)) - 5(8316) \\ &= 16(10\,920) - 16(8316) - 5(8316) \\ &= -21(8316) + 16(10\,920) \end{aligned}$$

This is our desired linear combination. Thus $m = -21$ and $n = 16$.

(*c*) By Theorem 11.15,

$$\text{lcm}\,(a, b) = \frac{|ab|}{\gcd(a, b)} = \frac{(8316)(10\,920)}{84} = 1\,081\,080$$

11.25. Let $a = 37$ and $b = 249$. (*a*) Find $d = \gcd(a, b)$. (*b*) Find integers m and n such that $d = ma + nb$. (*c*) Find $\text{lcm}\,(a, b)$.

(*a*) Divide the smaller number $a = 37$ into the larger number $b = 249$, and then repeatedly divide each remainder into the divisor until obtaining a zero remainder. These steps are pictured in Fig. 11-8. The last nonzero remainder is 1. Thus

$$\begin{array}{r|l} & 6 \\ 37 & 249 \\ & \underline{222} \\ & 27 \end{array} \qquad \begin{array}{r|l} & 1 \\ 27 & 37 \\ & \underline{27} \\ & 10 \end{array} \qquad \begin{array}{r|l} & 2 \\ 10 & 27 \\ & \underline{20} \\ & 7 \end{array} \qquad \begin{array}{r|l} & 1 \\ 7 & 10 \\ & \underline{7} \\ & 3 \end{array} \qquad \begin{array}{r|l} & 2 \\ 3 & 7 \\ & \underline{6} \\ & 1 \end{array} \qquad \begin{array}{r|l} & 1 \\ 1 & 3 \\ & \underline{3} \\ & 0 \end{array}$$

Fig. 11-8

(*b*) Now we find m and n such that

$$1 = 37m + 249n$$

The quotients in Fig. 11-8 (except the last) yield the following five equations:

(*1*) $27 = 249 - 6(37)$

(*2*) $10 = 37 - 1(27)$

(*3*) $7 = 27 - 2(10)$

(*4*) $3 = 10 - 1(7)$

(*5*) $1 = 7 - 2(3)$

Using (*5*) and (*4*), we write 1 as a linear combination of 7 and 10 as follows:

(*6*) $1 = 7 - 2(10 - 1(7)) = 7 - 2(10) + 2(7) = 3(7) - 2(10)$

Using (*6*) and (*3*), we write 1 as a linear combination of 10 and 27 as follows:

(*7*) $1 = 3(27 - 2(10)) - 2(10) = 3(27) - 6(10) - 2(10) = 3(27) - 8(10)$

Using (*7*) and (*2*), we write 1 as a linear combination of 27 and 37 as follows:

(*8*) $1 = 3(27) - 8(37 - 1(27)) = 3(27) - 8(37) + 8(27) = 11(27) - 8(37)$

Using (*8*) and (*1*), we write 1 as a linear combination of 37 and 249 as follows:

$$1 = 11(249 - 6(37)) - 8(37) = 11(249) - 66(37) - 8(37) = -74(37) + 11(249)$$

This is our desired linear combination. Thus $m = -74$ and $n = 11$.

(*c*) By Theorem 11.15,

$$\text{lcm}\,(a, b) = \frac{|ab|}{\text{gcd}\,(a, b)} = \frac{(37)(249)}{1} = 9213$$

11.26. Find the unique factorization of each number:

(*a*) 135; (*b*) 1330; (*c*) 3105, (*d*) 211

(*a*) $135 = 5 \cdot 27 = 5 \cdot 3 \cdot 3 \cdot 3$ or $135 = 3^3 \cdot 5$.

(*b*) $1330 = 2 \cdot 665 = 2 \cdot 5 \cdot 133 = 2 \cdot 5 \cdot 7 \cdot 19$.

(*c*) $3105 = 5 \cdot 621 = 5 \cdot 3 \cdot 207 = 5 \cdot 3 \cdot 3 \cdot 69 = 5 \cdot 3 \cdot 3 \cdot 3 \cdot 23$, or $3105 = 3^3 \cdot 5 \cdot 23$.

(*d*) None of the primes 2, 3, 5, 7, 11, 13 divides 211; hence 211 cannot be factored, that is, 211 is a prime. (Remark: We need only test those primes less than $\sqrt{211}$.)

11.27. Let $a = 2^3 \cdot 3^5 \cdot 5^4 \cdot 11^6 \cdot 17^3$ and $b = 2^5 \cdot 5^3 \cdot 7^2 \cdot 11^4 \cdot 13^2$. Find $\text{gcd}\,(a, b)$ and $\text{lcm}\,(a, b)$.

Those primes p_i which appear in both a and b will also appear in $\text{gcd}\,(a, b)$. Furthermore, the exponent of p_i in $\text{gcd}\,(a, b)$ will be the smaller of its exponents in a and b. Hence

$$\text{gcd}\,(a, b) = 2^3 \cdot 5^3 \cdot 11^4$$

Those primes p_i which appear in either a or b will also appear in $\text{lcm}\,(a, b)$. Also, the exponent of p_i in $\text{lcm}\,(a, b)$ will be the larger of its exponent in a and b. Hence

$$\text{lcm}\,(a, b) = 2^5 \cdot 3^5 \cdot 5^4 \cdot 7^2 \cdot 11^6 \cdot 13^2 \cdot 17^3$$

11.28. Prove Theorem 11.8: Suppose a, b, c are integers.

(i) If $a|b$ and $b|c$, then $a|c$.
(ii) If $a|b$ then, for any integer x, $a|bx$.
(iii) If $a|b$ and $a|c$, then $a|(b + c)$ and $a|(b - c)$.
(iv) If $a|b$ and $b \neq 0$, then $a = \pm b$ or $|a| < |b|$.
(v) If $a|b$ and $b|a$, then $|a| = |b|$, i.e., $a = \pm b$.
(vi) If $a|1$, then $a = \pm 1$.

(i) If $a|b$ and $b|c$, then there exist integers x and y such that $ax = b$ and $by = c$. Replacing b by ax, we obtain $axy = c$. Hence $a|c$.

(ii) If $a|b$, then there exists an integer c such that $ac = b$. Multiplying the equation by x, we obtain $acx = bx$. Hence $a|bx$.

(iii) If $a|b$ and $a|c$, then there exist integers x and y such that $ax = b$ and $ay = c$. Adding the equalities, we obtain

$$ax + ay = b + c \qquad \text{and so} \qquad a(x + y) = b + c$$

Hence $a|(b + c)$. Subtracting the equalities, we obtain

$$ax - ay = b - c \qquad \text{and so} \qquad a(x - y) = b - c.$$

Hence $a|(b - c)$.

(iv) If $a|b$, then there exists c such that $ac = b$. Then

$$|b| = |ac| = |a|\ |c|$$

By Problem 11.12(b), either $|c| = 1$ or $|a| < |a|\ |c| = |b|$. If $|c| = 1$, then $c = \pm 1$; whence $a = \pm b$, as required.

(v) If $a|b$, then $a = \pm b$ or $|a| < |b|$. If $|a| < |b|$, $b \nmid a$. Hence $a = \pm b$.

(vi) If $a|1$, then $a = \pm 1$ or $|a| < |1| = 1$. By Problem 11.12(a), $|a| \geq 1$. Therefore, $a = \pm 1$.

11.29. A nonempty subset J of $\mathbf{Z}$ is called an *ideal* if J has the following two properties:

(1) If $a, b \in J$, then $a + b \in J$.

(2) If $a \in J$ and $n \in Z$, then $na \in J$.

Let d be the least positive integer in an ideal $J \neq \{0\}$. Prove that d divides every element of J.

Since $J \neq \{0\}$, there exists $a \in J$ with $a \neq 0$. Then $-a = (-1)a \in J$. Thus J contains positive elements. By the well-ordering principle, J contains a least positive integer, so d exists. Now let $b \in J$. Dividing b by d, the division algorithm tells us there exist q and r such that

$$b = qd + r \qquad \text{and} \qquad 0 \leq r < d$$

Now, b, $d \in J$ and J is an ideal, hence $b + (-q)d = r$ also belongs to J. By the minimality of d, we must have $r = 0$. Hence $d|b$, as required.

11.30. Prove Theorem 11.12: Let d be the smallest positive integer of the form $ax + by$. Then $d = \gcd(a, b)$.

Consider the set $J = \{ax + yb: x, y \in \mathbf{Z}\}$. Then

$$a = 1(a) + 0(b) \in J \text{ and } b = 0(a) + 1(b) \in J$$

Also, suppose $s, t \in J$, say, $s = x_1a + y_1b$ and $t = x_2a + y_2b$. Then, for any $n \in \mathbf{Z}$,

$$s + t = (x_1 + x_2)a + (y_1 + y_2)b \qquad \text{and} \qquad ns = (nx_1)a + (ny_1)b$$

also belong to J. Thus J is an ideal. Let d be the least positive element in J. We claim $d = \gcd(a, b)$.

By the preceding Problem 11.28, d divides every element of J. Thus, in particular, d divides a and b. Now suppose h divides both a and b. Then h divides $xa + yb$ for any x and y; that is, h divides every element of J. Thus h divides d, and so $h \leq d$. Accordingly, $d = \gcd(a, b)$.

11.31. Prove Theorem 11.16: Suppose $\gcd(a, b) = 1$, and a and b divide c. Then ab divides c.

Since $\gcd(a, b) = 1$, there exist x and y such that $ax + by = 1$. Since $a|c$ and $b|c$, there exist m and n such that $c = ma$ and $c = nb$. Multiplying $ax + by = 1$ by c yields

$$acx + bcy = c \qquad \text{or} \qquad a(nb)x + b(ma)y = c \qquad \text{or} \qquad ab(nx + my) = c$$

Thus ab divides c.

11.32. Prove Corollary 11.18: Suppose a prime p divides a product ab. Then $p|a$ or $p|b$.

Suppose p does not divide a. Then $\gcd(p, a) = 1$ since the only divisors of p are ± 1 and $\pm p$. Thus there exist integers m and n such that $1 = mp + nq$. Multiplying by b yields $b = mpb + nab$. By hypothesis, $p|ab$, say, $ab = cp$. Then

$$b = mpb + nab = mpb + ncp = p(mb + nc).$$

Hence $p|b$, as required.

11.33. Prove: (*a*) Suppose $p|q$ where p and q are primes. Then $p = q$. (*b*) Suppose $p|q_1q_2 \cdots q_r$ where p and the q's are primes. Then p is equal to one of the q's.

(*a*) The only divisors of q are ± 1 and $\pm q$. Since $p > 1$, $p = q$.

(*b*) If $r = 1$, then $p = q_1$ by (*a*). Suppose $r > 1$. By Problem 11.32 (Corollary 11.18), $p|q_1$ or $p|(q_2 \cdots q_r)$. If $p|q_1$, then $p = q_1$ by (*a*). If not, then $p|(q_2 \cdots q_r)$. We repeat the argument. That is, we get $p = q_2$ or $p|(q_3 \cdots q_r)$. Finally (or by induction) p must equal one of the q's.

11.34. Prove the Fundamental Theorem of Arithmetic (Theorem 11.19): Every integer $n > 1$ can be expressed uniquely (except for order) as a product of primes.

We already proved Theorem 11.10 that such a product of primes exists. Hence we need only show that such a product is unique (except for order). Suppose

$$n = p_1p_2 \cdots p_k = q_1q_2 \cdots q_r$$

where the p's and q's are primes. Note that $p_1|(q_1 \cdots q_r)$. By the preceding Problem 11.33, p_1 equals one of the q's. We rearrange the q's so that $p_1 = q_1$. Then

$$p_1p_2 \cdots p_k = p_1q_2 \cdots q_r \qquad \text{and so} \qquad p_2 \cdots p_k = q_2 \cdots q_r$$

By the same argument, we can rearrange the remaining q's so that $p_2 = q_2$. And so on. Thus n can be expressed uniquely as a product of primes (except for order).

CONGRUENCES

11.35. Which of the following are true?

(*a*) $446 \equiv 278 \pmod 7$. (*d*) $473 \equiv 369 \pmod{26}$.

(*b*) $793 \equiv 682 \pmod 9$. (*e*) $445 \equiv 536 \pmod{18}$.

(*c*) $269 \equiv 413 \pmod{12}$. (*f*) $383 \equiv 126 \pmod{15}$.

Recall $a \equiv b \pmod m$ if and only if m divides $a - b$.

(*a*) **Method 1**: Find the difference $446 - 278 = 168$. Divide the difference 168 by the modulus $m = 7$. The remainder is 0; hence the statement is true.

Method 2: Reduce each side modulo 7. Dividing 446 by 7 gives a remainder $r = 5$, and dividing 278 by 7 also gives a remainder $r = 5$. Hence $446 \equiv 278 \pmod 7$.

(*b*) Divide the difference $793 - 682 = 111$ by the modulus $m = 9$. The remainder is not 0; hence the statement is false. (Alternatively, dividing 793 by 9 yields a remainder $r = 1$, but dividing 682 by 9 yields a remainder $r = 6$.)

(*c*) True; since 12 divides $269 - 413 = -144$.

(*d*) True; since 26 divides $472 - 359 = 104$.

(*e*) False; since 18 does not divide $445 - 536 = -91$.

(*f*) False; since 15 does not divide $383 - 126 = 157$.

11.36. Find the smallest nonnegative integer which is congruent modulo $m = 8$ to each of the following numbers: (*a*) 379; (*b*) 695; (*c*) -578; (*d*) -285.

[The integer should be in the set $\{0, 1, 2, \ldots, 7\}$.]

(*a*) Dividing 379 by $m = 8$ yields a remainder 3; hence

$$379 \equiv 3 \pmod 8$$

(*b*) Dividing 695 by $m = 8$ yields a remainder 7; hence

$$695 \equiv 7 \pmod 8$$

(*c*) Dividing 578 by $m = 8$ yields a remainder 2; hence

$$-578 \equiv -2 \equiv 6 \pmod 8$$

(We obtain 6 by adding the modulus $m = 8$ to -2.)

(*d*) Dividing 285 by $m = 8$ yields a remainder 5; hence

$$-285 \equiv -5 \equiv 3 \pmod 8$$

11.37. Find the smallest integer in absolute value which is congruent modulo $m = 7$ to each of the following numbers:

(*a*) 386; (*b*) 257; (*c*) -192; (*d*) -466.

[The integer should be in the set $\{-3, -2, -1, 0, 1, 2, 3\}$.]

(*a*) Dividing 386 by $m = 7$ yields a remainder 1; hence

$$386 = 1 \pmod 7$$

(*b*) Dividing 257 by $m = 7$ yields a remainder 5; hence

$$257 \equiv 5 \equiv -2 \pmod 7$$

(We obtain -2 by subtracting the modulus $m = 7$ from 5.)

(*c*) Dividing 192 by $m = 7$ yields a remainder 3; hence

$$-192 \equiv -3 \pmod 7$$

(*b*) Dividing 466 by $m = 7$ yields a remainder 4; hence

$$-466 \equiv -4 \equiv 3 \pmod 7$$

(We obtain 3 by adding the modulus $m = 7$ to -4.)

11.38. Find all numbers between 1 and 100 which are congruent to 6 modulo $m = 13$, that is, find all x such that $1 \leq x \leq 100$ and

$$x \equiv 6 \pmod{13}$$

Add multiples of the modulus $m = 13$ to the given number 6 to obtain:

$$6 + 0 = 6, \quad 6 + 13 = 19, \quad 19 + 13 = 32, \quad 32 + 13 = 45$$
$$45 + 13 = 58, \quad 58 + 13 = 71, \quad 71 + 13 = 84, \quad 84 + 13 = 97$$

That is,

$$6, \quad 19, \quad 32, \quad 45, \quad 58, \quad 71, \quad 84, \quad 97$$

11.39. Find all numbers between -50 and 50 which are congruent to 21 modulo $m = 12$, that is, find all x such that $-50 \leq x \leq 50$ and

$$x \equiv 21 \pmod{12}$$

Add and subtract multiples of the modulus $m = 12$ to the given number 21 to obtain:

$$21 + 0 = 21, \quad 21 + 12 = 33, \quad 33 + 12 = 46, \quad 21 - 12 = 9$$
$$9 - 12 = -3, \quad -3 - 12 = -15, \quad -15 - 12 = -27, \quad -27 - 12 = -39$$

That is,

$$-39, \quad -27, \quad -15, \quad -3, \quad 9, \quad 21, \quad 33, \quad 46$$

11.40. Prove Theorem 11.20: Let m be a positive integer. Then:

(i) For any integer a, we have $a \equiv a \pmod{m}$.

(ii) If $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$.

(iii) If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.

(i) The difference $a - a = 0$ is divisible by m; hence $a \equiv a \pmod{m}$.

(ii) If $a \equiv b \pmod{m}$, then $m|(a-b)$. Hence m divides $-(a-b) = b - a$. Therefore, $b \equiv a \pmod{m}$.

(iii) We are given $m|(a-b)$ and $m|(b-c)$. Hence m divides the sum $(a-b)+(b-c) = a-c$. Therefore, $a \equiv c \pmod{m}$.

11.41. Prove Theorem 11.21: Suppose $a \equiv c \pmod{m}$ and $b \equiv d \pmod{m}$. Then:

(i) $a + b \equiv c + d \pmod{m}$.

(ii) $a \cdot b \equiv c \cdot d \pmod{m}$.

We are given that $m|(a-c)$ and $m|(b-d)$.

(i) Then m divides the sum $(a-c)+(b-d) = (a+b)-(c+d)$. Hence

$$a + b \equiv c + d \pmod{m}$$

(ii) Then m divides the product $b(a-c) = ab - bc$ and m divides the product $c(b-d) = bc - cd$. Thus m divides the sum

$$(ab - bc) + (bc - cd) = ab - cd$$

Thus $ab \equiv cd \pmod{m}$.

11.42. Prove: If $a + b \equiv a + c \pmod{m}$, then $b \equiv c \pmod{m}$.

(That is, the cancelation law holds for addition modulo m.)

By hypothesis, m divides the difference $(a+b)-(a+c) = b - c$. Hence $b \equiv c \pmod{m}$, as required.

11.43. Let $d = \gcd(a, b)$. Show that a/d and b/d are relatively prime.

There exists x and y such that $d = xa + yb$. Dividing the equation by d, we get $1 = x(a/d) + y(b/d)$. Hence a/d and b/d are relatively prime.

11.44. Prove Theorem 11.23: Suppose $ab \equiv ac \pmod{m}$ and $d = \gcd(a, m)$. Then $b \equiv c \pmod{m/d}$.

By hypothesis, m divides $ab - ac = a(b-c)$. Hence, there is an integer x such that $a(b-c) = mx$. Dividing by d yields

$$(a/d)(b-c) = (m/d)x$$

Thus m/d divides $(a/d)(b-c)$. Since m/d and a/d are relatively prime, m/d divides $b - c$. That is, $b \equiv c \pmod{m/d}$, as required.

RESIDUE SYSTEMS, EULER PHI FUNCTION f

11.45. For each modulo m, exhibit two complete residue systems, one consisting of the smallest non-negative integers, and the other consisting of the integers with the smallest absolute values:

$$(a)\ m = 9; \quad (b)\ m = 12.$$

In the first case choose $\{0, 1, 2, \ldots, m-1\}$, and in the second case choose

$$\{-(m-1)/2, \ldots, -1, 0, 1, \ldots, (m-1)/2\} \qquad \text{or} \qquad \{-(m-2)/2, \ldots, -1, 0, 1, \ldots, m/2\}$$

according as m is even or odd:

(*a*) $\{0, 1, 2, 3, 4, 5, 6, 7, 8\}$ and $\{-4, -3, -2, -1, 0, 1, 2, 3, 4\}$.

(*b*) $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$ and $\{-5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6\}$.

11.46. Exhibit a reduced residue system modulo m and find $\phi(m)$ where: (*a*) $m = 9$; (*b*) $m = 12$; (*c*) $m = 13$; (*d*) $m = 16$.

Choose those positive numbers less than m and relatively prime to m. The number of such numbers is $\phi(m)$.

(*a*) $\{1, 2, 4, 5, 7, 8\}$; hence $\phi(9) = 6$.

(*b*) $\{1, 5, 7, 11\}$; hence $\phi(12) = 4$.

(*c*) $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$; hence $\phi(13) = 12$. [This is expected since $\phi(p) = p - 1$ for any prime p.]

(*d*) $\{1, 3, 5, 7, 9, 11, 13, 15\}$; hence $\phi(16) = 8$.

11.47. Recall $S_m = \{0, 1, 2, \ldots, m-1\}$ is a complete residue system modulo m. Prove:

(*a*) Any m consecutive integers is a complete residue system modulo m.

(*b*) If $\gcd(a, m) = 1$, then $aS_m = \{0, a, 2a, 3a, \ldots, (m-1)a\}$ is a complete residue system modulo m.

(*a*) Consider any other sequence of m integers, say

$$\{a, a+1, a+2, \ldots, a+(m-1)\}$$

The absolute value of the difference s of any two of the integers is less than m. Thus m does not divide s, and so the numbers are incongruent modulo m.

(*b*) Suppose $ax \equiv ay \pmod{m}$ where $x, y \in S_m$. Since $\gcd(a, m) = 1$, the modified cancelation law Theorem 11.23 tells us $x \equiv y \pmod{m}$. Since $x, y \in S_m$, we must have $x = y$. That is, aS_m is a complete residue system modulo m.

11.48. Exhibit a complete residue system modulo $m = 8$ consisting entirely of multiples of 3.

By Problem 11.47(*b*), $3S_8 = \{0, 3, 6, 9, 12, 15, 18, 21\}$ is a complete residue system modulo $m = 8$.

11.49. Show that if p is a prime, then

$$\phi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1)$$

Clearly, $\gcd(a, p^n) \neq 1$ if and only if p divides a. Thus the only numbers between 1 and p^n which are not relatively prime to p^n are the multiples of p, that is,

$$p, \quad 2p, \quad 3p, \quad \ldots, \quad p^{n-1}(p)$$

There are p^{n-1} such multiples of p. All the other numbers between 1 and p^n are relatively prime to p^n. Thus

$$\phi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1)$$

as claimed.

11.50. Find: (*a*) $\phi(81), \phi(125), \phi(7^6)$; (*b*) $\phi(72), \phi(3000)$.

(*a*) By Problem 11.49,

$$\phi(81) = \phi(3^4) = 3^3(2-1) = 27(2) = 54$$
$$\phi(125) = \phi(5^3) = 5^2(5-1) = 25(4) = 100$$
$$\phi(7^6) = 7^5(7-1) = 6(7^5)$$

(*b*) Use Theorem 11.24 that ϕ is multiplicative.

$$\phi(72) = \phi(3^2 \cdot 2^3) = \phi(3^2)\phi(2^3) = 3(3-1) \cdot 2^2(2-1) = 24$$
$$\phi(3000) = \phi(3 \cdot 2^2 \cdot 5^3) = \phi(3)\phi(2^2)\phi(5^3) = 2 \cdot 2 \cdot 5^2(5-1) = 400$$

11.51. Prove Theorem 11.24: If a and b are relatively prime, then $\phi(ab) = \phi(a)\phi(b)$.

Let a and b be coprime (relatively prime) positive integers, and let S be the set of numbers from 1 to ab arranged in an array as in Fig. 11-9. That is, the first row of S is the list of numbers from 1 to a, the second row is the list of numbers from $a+1$ to $2a$, and so on. Since a and b are coprime, any integer x is coprime to ab if and only if it is coprime to both a and b. We find the number of such integers x in the array S.

Since $na + k \equiv k \pmod{a}$, each column in S belongs to the same residue class modulo a. Therefore, any integer x in S is coprime to a if and only if x belongs to a column headed by an integer k which is coprime to a. Thus there are $\phi(a)$ such columns since the first row is a residue system modulo a.

1	2	3	$\ldots$	k	$\ldots$	a
$a+1$	$a+2$	$a+3$	$\ldots$	$a+k$	$\ldots$	$2a$
$2a+1$	$2a+2$	$2a+3$	$\ldots$	$2a+k$	$\ldots$	$3a$
$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$
$(b-1)a+1$	$\ldots$	$\ldots$	$\ldots$	$(b-1)a+k$	$\ldots$	ba

Fig. 11-9

Now let us consider an arbitrary column in the array S which consists of the numbers

$$k, \quad a+k, \quad 2a+k, \quad 3a+k, \ \ldots, \ (b-1)a+k \qquad (*)$$

We claim that these b integers from a residue system modulo b, that is, no two of the integers are congruent modulo b. Suppose

$$na + k \equiv n'a + k \pmod{b} \qquad \text{and so} \qquad na \equiv n'a \pmod{b}$$

But a and b are coprime, and so by the modified cancelation law

$$n \equiv n' \pmod{b}$$

However, n and n' belong to $\{0, 1, 2, \ldots, b-1\}$. Thus $n = n'$ and $(*)$ is a complete residue system modulo b. Therefore, $(*)$ contains exactly $\phi(b)$ integers which are coprime to b.

We have shown that the array S contains $\phi(a)$ columns consisting of those integers which are coprime to a, and each such column contains $\phi(b)$ integers which are coprime to b. Thus there are $\phi(a)\phi(b)$ integers in the array S which are coprime to both a and b and hence are coprime to ab. Accordingly,

$$\phi(ab) = \phi(a)\phi(b)$$

as required.

ARITHMETIC MODULO m, $\mathbf{Z}_m$

11.52. Exhibit the addition and multiplication tables for: (*a*) $\mathbf{Z}_4$; (*b*) $\mathbf{Z}_7$.

(*a*) See Fig. 11-10. (*b*) See Fig. 11-11.

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

×	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Fig. 11-10

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

×	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Fig. 11-11

11.53. In $\mathbf{Z}_{11}$, find: (*a*) $-2, -3, -5, -8, -9, -10$; (*b*) 2/7, 3/7, 5/7, 8/7, 10/7, 1/7.

(*a*) Note $-a = m - a$ since $(m - a) + a = 0$. Therefore:

$$-2 = 11 - 2 = 9, \qquad -5 = 11 - 5 = 6, \qquad -9 = 11 - 9 = 2$$
$$-3 = 11 - 3 = 8, \qquad -8 = 11 - 8 = 3, \qquad -10 = 11 - 10 = 1$$

(*b*) By definition a/b is the integer c such that $bc = a$. Since we are dividing by 7, first compute the multiplication table for 7 in $\mathbf{Z}_{11}$; that is,

×	0	1	2	3	4	5	6	7	8	9	10
7	0	7	3	10	6	2	9	5	1	8	4

Now find the number inside the table, and the answer will be above this number. Thus:

$$2/7 = 5, \qquad 3/7 = 2, \qquad 5/7 = 7, \qquad 8/7 = 9, \qquad 10/7 = 3, \qquad 1/7 = 8$$

[Note that $7^{-1} = 8$ since $7(8) = 8(7) = 1$.]

11.54. Consider $\mathbf{Z}_p$ where p is a prime. Prove:

(*a*) If $ab = ac$ and $a \neq 0$, then $b = c$.

(*b*) If $ab = 0$, then $a = 0$ or $b = 0$.

(*a*) If $ab = ac$ in $\mathbf{Z}_p$, then $ab \equiv ac \pmod{p}$. Since $a \neq 0$, $\gcd(a, p) = 1$. By Theorem 11.22, we can canel the a's to obtain

$$b \equiv c \pmod{p}$$

Therefore $b = c$ in $\mathbf{Z}_p$.

(*b*) If $ab = 0$ in $\mathbf{Z}_p$, then $ab \equiv 0 \pmod{p}$. Therefore, p divides the product ab. Since p is a prime, $p|a$ or $p|b$; that is,

$$a \equiv 0 \pmod{p} \qquad \text{or} \qquad b \equiv 0 \pmod{p}$$

Thus $a = 0$ or $b = 0$ in $\mathbf{Z}_p$.

11.55. Consider $a \neq 0$ in $\mathbf{Z}_m$ where $\gcd(a, m) = 1$. Show that a has a multiplicative inverse in $\mathbf{Z}_m$.

Since $a \neq 0$ and $\gcd(a, m) = 1$, there exists integers x and y such that $ax + my = 1$ or $ax - 1 = my$. Thus m divides $ax - 1$ and hence $ax \equiv 1 \pmod{m}$. Reduce x modulo m to an element x' in $\mathbf{Z}_m$. Then $ax' = 1$ in $\mathbf{Z}_m$.

11.56. Find a^{-1} in $\mathbf{Z}_m$ where (*a*) $a = 37$ and $m = 249$; (*b*) $a = 15$ and $m = 234$.

(*a*) Find $d = \gcd(37, 249)$, as in Problem 11.25. Since $d = \gcd(37, 249) = 1$, a^{-1} does exist. Find integers x and y such that $37x + 249y = 1$. By Problem 11.25,

$$-74(37) + 11(249) = 1 \qquad \text{so} \qquad -74(37) \equiv 1 \pmod{249}$$

Add $m = 249$ to -74 to obtain $-74 + 249 = 175$. Thus

$$(175)(37) \equiv 1 \pmod{249}$$

Thus $a^{-1} = 175$ in $\mathbf{Z}_{249}$.

(*b*) Find $d = \gcd(15, 234) = 3$. Thus $d \neq 1$, and hence 15 has no multiplicative inverse in $\mathbf{Z}_{234}$.

11.57. Consider the following polynomials over $\mathbf{Z}_7$:

$$f(x) = 6x^3 - 5x^2 + 2x - 4, \qquad g(x) = 5x^3 + 2x^2 + 6x - 1, \qquad h(x) = 3x^2 - 2x - 5$$

Find: (*a*) $f(x) + g(x)$; (*b*) $f(x)h(x)$.

Perform the operations as if the polynomials were over the integers $\mathbf{Z}$, and then reduce the coefficients modulo 7.

(*a*) We have:

$$\begin{array}{r} 6x^3 - 5x^2 + 2x - 4 \\ \underline{5x^3 + 2x^2 + 6x - 4} \\ 11x^3 - 3x^2 + 8x - 5 \end{array} \qquad \text{or} \qquad 4x^3 - 3x^2 + x - 5 \qquad \text{or} \qquad 4x^3 + 4x^2 + x + 2$$

(*b*) We have:

$$\begin{array}{r} 6x^3 - 5x^2 + 2x - 4 \\ \underline{3x^2 - 2x \ - 5} \\ 18x^5 - 15x^4 + \ 6x^3 - 12x^2 \\ \quad - 12x^4 + 10x^3 - \ 4x^2 + \ 8x \\ \quad\quad - 30x^2 + 25x^2 - 10x + 20 \\ \hline 18x^5 - 27x^4 + 14x^3 + 9x^2 \ - \ 2x + 20 \end{array}$$

$$\text{or} \quad 4x^5 - \ 6x^4 \qquad + 2x^2 \ - \ 2x + \ 6$$

$$\text{or} \quad 4x^5 + x^4 + 2x^2 + 5x + 6$$

CONGRUENCE EQUATIONS

11.58. Solve the congruence equation $f(x) = 4x^4 - 3x^3 + 2x^2 + 5x - 4 \equiv 0 \pmod 6$.

Since the equation is not linear, we solve the equation by testing the numbers in a complete residue system modulo 6, say,

$$\{0, 1, 2, 3, 4, 5\}$$

We have:

$$\begin{aligned}
f(0) &= -4 \not\equiv 0 \pmod 6 \\
f(1) &= 4 - 3 + 2 + 5 - 4 = 4 \not\equiv 0 \pmod 6 \\
f(2) &= 64 - 24 + 8 + 10 - 4 = 54 \equiv 0 \pmod 6 \\
f(3) &= 324 - 81 + 18 + 15 - 4 = 272 \equiv 2 \not\equiv 0 \pmod 6 \\
f(4) &= 1024 - 192 + 32 + 20 - 4 = 880 \equiv 4 \not\equiv 0 \pmod 6 \\
f(5) &= 2500 - 375 + 50 + 25 - 4 = 2196 \equiv 0 \pmod 6
\end{aligned}$$

Thus only 2 and 5 are roots of $f(x)$ modulo 6. That is, $\{2, 5\}$ is a complete set of solutions.

11.59. Solve the congruence equation

$$f(x) = 26x^4 - 31x^3 + 46x^2 - 76x + 57 \equiv 0 \pmod 8$$

First we reduce the coefficients of $f(x)$ modulo 8 to obtain the equivalent congruence equation

$$g(x) = 2x^4 - 7x^3 + 6x^2 - 4x + 1 \equiv 0 \pmod 8$$

Since $7 \equiv -1 \pmod 8$ and $6 \equiv -2 \pmod 8$, we can further simplify our original equation to obtain the equivalent congruence equation

$$h(x) = 2x^4 + x^3 - 2x^2 - 4x + 1 \equiv 0 \pmod 8$$

We test the numbers in a complete residue system modulo 8 and, in order to keep our arithmetic as simple as possible, we choose

$$\{-3, -2, -1, 0, 1, 2, 3, 4\}$$

(That is, we chose those numbers whose absolute value is minimal.) Substituting these numbers in $h(x)$ we obtain:

$$\begin{aligned}
h(-3) &= 130 \equiv 2 \pmod 8, & h(1) &= -2 \equiv 6 \pmod 8 \\
h(-2) &= 25 \equiv 1 \pmod 8, & h(2) &= 25 \equiv 1 \pmod 8 \\
h(-1) &= 94 \equiv 4 \pmod 8, & h(3) &= 160 \equiv 0 \pmod 8 \\
h(0) &= 91 \equiv 1 \pmod 8, & h(4) &= 513 \equiv 1 \pmod 8
\end{aligned}$$

Therefore, 3 is the only solution of $f(x) \pmod 8$.

11.60. Solve each linear congruence equation:

(*a*) $3x \equiv 2 \pmod 8$; (*b*) $6x \equiv 5 \pmod 9$; (*c*) $4x \equiv 6 \pmod{10}$

Since the moduli are relatively small, we find all the solutions by testing. Recall $ax \equiv b \pmod m$ has exactly $d = \gcd(a, m)$ solution providing d divides b.

(*a*) Here $\gcd(3, 8) = 1$, hence the equation has a unique solution. Testing $0, 1, 2, \ldots, 7$, we find that

$$3(6) = 18 \equiv 2 \pmod 8$$

(*b*) Here $\gcd(6, 9) = 3$, but 3 does not divide 5. Hence the system has no solution.

(*c*) Here $\gcd(4, 10) = 2$ and 2 divides 6; hence the system has two solutions.

Method 1: Testing $0, 1, 2, 3, \ldots, 9$, we see that

$$4(4) = 16 \equiv 6 \pmod{10} \qquad \text{and} \qquad 4(9) = 36 \equiv 6 \pmod{10}$$

Hence 4 and 9 are our two solutions.

Method 2: Divide the equation and the modulus by $\gcd(4, 10) = 2$ to obtain the congruence equation

$$2x \equiv 3 \pmod{5}$$

This has the unique solution $x = 4$ which is a solution of the original equation. Add the new modulus 5 to this solution to get

$$x = 4 + 5 = 9$$

which is the second solution of the original equation. Hence 4 and 9 are our two solutions.

11.61. Solve the congruence equation $1092x \equiv 213 \pmod{2295}$.

Testing is not an efficient way to solve this equation since the modulus $m = 2295$ is large. First use the division algorithm to find $d = \gcd(1092, 2295) = 3$. Dividing 213 by $d = 3$ yields 0 as a remainder; that is, 3 does divide 213. Thus the equation will have three (incongruent) solutions.

Divide the equation and the modulus $m = 2295$ by $d = 3$ to obtain the congruence equation

$$364x \equiv 71 \pmod{765} \qquad (*)$$

We know that 364 and 796 are relatively prime since we divided by $d = \gcd(1092, 2295) = 3$; hence the equation $(*)$ has a unique solution modulo 765. We solve $(*)$ by first finding the solution of the equation

$$364x \equiv 1 \pmod{765} \qquad (**)$$

This solution is obtained by finding s and t such that

$$364s + 765t = 1$$

This is done by using the division algorithm and "unraveling" (as in Problem 11.25).

$$\begin{array}{r|l} & 2 \\ 364 & \overline{765} \\ & \underline{728} \\ & 37 \end{array} \qquad \begin{array}{r|l} & 9 \\ 37 & \overline{364} \\ & \underline{333} \\ & 31 \end{array} \qquad \begin{array}{r|l} & 1 \\ 31 & \overline{37} \\ & \underline{31} \\ & 6 \end{array} \qquad \begin{array}{r|l} & 5 \\ 6 & \overline{31} \\ & \underline{30} \\ & 1 \end{array}$$

Fig. 11-12

Specifically, divide $a = 364$ into $m = 765$, and repeatedly divide each remainder into the divisor as in Fig. 11-12. The quotients in Fig. 11-12 yield the following four equations:

(*1*) $37 = 765 - 2(364)$

(*2*) $31 = 364 - 9(37)$

(*3*) $6 = 37 - 1(31)$

(*4*) $1 = 31 - 5(6)$

Using (*4*) and (*3*), write 1 as a linear combination of 31 and 37 as follows:

(*5*) $1 = 31 - 5[37 - 1(31)] = 6(31) - 5(37)$

Using (*5*) and (*2*), write 1 as a linear combination of 364 and 37 as follows:

(*6*) $1 = 6[364 - 9(37)] - 5(37) = 6(364) - 59(37)$

Using (*6*) and (*1*), write 1 as a linear combination of 364 and 795 as follows:

(*7*) $1 = 6(364) - 59[765 - 2(364)] = 124(364) - 59(765)$

Thus $s = 124$ and $t = -59$.

Accordingly, $s = 124$ is the unique solution of $(**)$. Multiplying this solution $s = 124$ by 71 and reducing modulo 765 we obtain

$$124(71) = 8804 \equiv 389 \pmod{765}$$

This is the unique solution of $(*)$.

Lastly, we add the new modulus $m = 765$ to the solution $x_1 = 389$ two times to obtain the other two solutions of the given equation:

$$x_2 = 389 + 765 = 1154, \qquad x_3 = 1154 + 765 = 1919$$

In other words, $x_1 = 389$, $x_2 = 1154$, $x_3 = 1919$ form a complete set of solutions of the given equation $1092x \equiv 213 \pmod{2295}$.

11.62. Solve the congruence equation $455x \equiv 204 \pmod{469}$.

First use the division algorithm to find $d = \gcd(455, 469) = 7$. Dividing 204 by $d = 7$ yields 1 as a remainder; that is, 7 does not divide 204. Thus the equation has no solution.

11.63. A boy sells apples for 12 cents each and pears for 7 cents each. Suppose the boy collected \$3.21. How many apples and pears did he sell?

Let x denote the number of apples sold and y the number of pears sold. This gives the diophantine equation

$$12x + 7y = 321 \qquad (*)$$

(It is a *diophantine equation* since x and y are restricted to nonnegative integers.] The equation $(*)$ is equivalent to the congruence equation

$$12x \equiv 321 \pmod{7}$$

Reducing this equation modulo 7 we obtain the equivalent equation

$$5x \equiv 6 \pmod{7}$$

Testing $0, 1, \ldots, 6$, we obtain the unique solution

$$x = 4$$

We add multiples of the modulus $m = 7$ to 4 to obtain the possible values of x and in each case we substitute in $(*)$ to obtain the corresponding value of y. This yields

$$x = 4,\ y = 39; \qquad x = 11,\ y = 27; \qquad x = 18,\ y = 15$$

Since $12(25) = 400$ is larger than 321, $x = 25$ and any larger value for x will yield a negative value of y. Accordingly, there are three possible solutions:

$$4 \text{ apples, } 39 \text{ pears}; \qquad 11 \text{ apples, } 27 \text{ pears}; \qquad 18 \text{ apples, } 15 \text{ pears}$$

In other words,

$$x = 4 + 7t \qquad \text{and} \qquad y = 39 - 12t$$

is the general solution of $(*)$, and $t = 0, 1, 2$ are the only values of t which yield nonnegative values for both x and y.

11.64. Find the smallest positive integer x such that when x is divided by 3 it yields a remainder 2, when x is divided by 7 it yields a remainder 4, and when x is divided by 10 it yields a remainder 6?

We seek the smallest positive common solution of the following three congruence equations:

$$(a)\quad x \equiv 2 \pmod{3}; \qquad (b)\quad x \equiv 4 \pmod{7}; \qquad (c)\quad x \equiv 6 \pmod{10}$$

Observe that the moduli 3, 7, and 10 are pairwise relatively prime. (Moduli is the plural of modulus.) The Chinese Remainder Theorem (CRT) 11.28 tells us that there is a unique solution modulo the product $m = 3(7)(10) = 210$. We solve the problems in two ways.

Method 1: First we apply CRT to the first two equations,

$$(a) \quad x \equiv 2 \pmod 3 \qquad \text{and} \qquad (b) \quad x \equiv 4 \pmod 7$$

We know there is a unique solution modulo $M = 3 \cdot 7 = 21$. Adding multiples of the modulus $m = 7$ to the given solution $x = 4$ of the second equation (b), we obtain the following three solutions of (b) which are less than 21:

$$4, \quad 11, \quad 18$$

Testing each of these solutions of (b) in the first equation (a), we find that 11 is the only solution of both equations.

Now we apply the same process to the two equations

$$(c) \quad x \equiv 6 \pmod{10} \qquad \text{and} \qquad (d) \quad x \equiv 11 \pmod{21}$$

CRT tells us there is a unique solution modulo $M = 21 \cdot 10 = 210$. Adding multiples of the modulus $m = 21$ to the given solution $x = 11$ of the equation (d), we obtain the following 10 solutions of (d) which are less than 210:

$$11, \quad 32, \quad 53, \quad 74, \quad 95, \quad 116, \quad 137, \quad 158, \quad 179, \quad 210$$

Testing each of these solutions of (d) in the equation (c), we find that $x = 116$ is the only solution of equation (c). Thus

$$x = 116$$

is the smallest positive integer satisfying all of the three given equations (a), (b), and (c),

Method 2: Using the notation of Proposition 11.29, we obtain

$$M = 3 \cdot 7 \cdot 10 = 210, \qquad M_1 = 210/3 = 70, \qquad M_2 = 210/7 = 30, \qquad M_3 = 210/10 = 21$$

We now seek solutions to the equations

$$70x \equiv 1 \pmod 3, \qquad 30x \equiv 1 \pmod 7, \qquad 21x \equiv 1 \pmod{10}$$

Reducing 70 modulo 3, reducing 30 modulo 7, and reducing 21 modulo 10, we obtain the equivalent system

$$x \equiv 1 \pmod 3, \qquad 2x \equiv 1 \pmod 7, \qquad x \equiv 1 \pmod{10}$$

The solutions of these three equations are, respectively,

$$s_1 = 1, \qquad s_2 = 4, \qquad s_3 = 1$$

Substituting into the formula

$$x_0 = M_1 s_1 r_1 + M_2 s_2 r_2 + \cdots + M_k s_k r_k$$

we obtain the following solution of our original system:

$$x_0 = 70 \cdot 1 \cdot 2 \quad + \quad 30 \cdot 4 \cdot 4 \quad + \quad 21 \cdot 1 \cdot 6 = 746$$

Dividing this solution by the modulus $M = 210$, we obtain the remainder

$$x = 116$$

which is the unique solution of the original system between 0 and 210.

11.65. Prove Theorem 11.25: If a and m are relatively prime, then $ax \equiv 1 \pmod{m}$ has a unique solution; otherwise it has no solution.

Suppose x_0 is a solution. Then m divides $ax_0 - 1$, and hence there exists y_0 such that $my_0 = ax_0 - 1$. Therefore

$$ax_0 + my_0 = 1 \tag{1}$$

and a and m are coprime (relatively prime). Conversely, if a and m are coprime, then there exist x_0 and y_0 satisfying (*1*), in which case x_0 is a solution of $ax \equiv 1 \pmod{m}$.

It remains to prove that x_0 is a unique solution modulo m. Suppose x_1 is another solution. Then

$$ax_0 \equiv 1 \equiv ax_1 \pmod{m}$$

Since a and m are coprime, the Modified Cancelation Law holds here, so

$$x_0 \equiv x_1 \pmod{m}$$

Thus the theorem is proved.

11.66. Prove Theorem 11.26: Suppose a and m are relatively prime. Then $ax \equiv b \pmod{m}$ has a unique solution. Moreover, if s is the unique solution of $ax \equiv 1 \pmod{m}$, then $x = bs$ is the unique solution to $ax \equiv b \pmod{m}$.

By Theorem 11.25 (proved in Problem 11.65), a unique solution s of $ax \equiv 1 \pmod{m}$ exists. Hence $as \equiv 1 \pmod{m}$ and so

$$a(bs) = (as)b \equiv 1 \cdot b = b \pmod{m}$$

That is, $x = bs$ is a solution of $ax \equiv b \pmod{m}$. Suppose x_0 and x_1 are two such solutions. Then

$$ax_0 \equiv b \equiv ax_1 \pmod{m}$$

Since a and m are coprime, the Modified Cancelation Law tells us that $x_0 \equiv x_1 \pmod{m}$. That is, $ax \equiv b \pmod{m}$ has a unique solution modulo m.

11.67. Prove Theorem 11.27: Consider the equation

$$ax \equiv b \pmod{m} \tag{$*$}$$

where $d = \gcd(a, m)$. (i) If d does not divide b, then Eq. $(*)$ has no solution. (ii) If d does divide b, then Eq. $(*)$ has d solutions which are all congruent modulo M to the unique solution of

$$Ax \equiv B \pmod{M} \tag{$**$}$$

where $A = a/d$, $B = b/d$, and $M = m/d$.

(i) Suppose x_0 is a solution of $(*)$. Then $ax_0 \equiv b \pmod{m}$, and so m divides $ax_0 - b$. Thus there exists an integer y_0 such that $my_0 = ax_0 - b$ or $my_0 + ax_0 = b$. But $d = \gcd(a, m)$, and so d divides $my_0 + ax_0$. That is, d divides b. Accordingly, if d does not divide b, then no solution exists.

(ii) Suppose x_0 is a solution of $(*)$. Then, as above,

$$my_0 + ax_0 = b$$

Dividing through by d we get $(**)$. Hence M divides $Ax_0 - B$ and so x_0 is a solution of $(**)$. Conversely, suppose x_1 is a solution of $(**)$. Then, as above, there exists an integer y_1 such that

$$My_1 + Ax_1 = B$$

Multiplying through by d yields

$$dMy_1 + dAx_1 = dB \qquad \text{or} \qquad my_1 + ax_1 = b$$

Therefore m divides $ax_1 - b$, whence x_i is a solution of $(*)$. Thus $(**)$ have the same integer solution. Let x_0 be the unique smallest positive solutions of $(**)$. Since $m = dM$,

$$x_0, \quad x_0 + M, \quad x_0 + 2M, \quad x_0 + 3M, \quad \ldots, \quad x_0 + (d-1)M$$

are precisely the solutions of $(**)$ and $(*)$ between 0 and m. Thus $(*)$ has d solutions modulo m, and all are congruent to x_0 modulo M.

11.68. Prove the Chinese Remainder Theorem (Theorem 11.28:) Given the system

$$x \equiv r_1 \pmod{m_1}, \qquad x \equiv r_2 \pmod{m_2}, \qquad \ldots, \qquad x \equiv r_k \pmod{m_k} \tag{1}$$

where the m_i are pairwise relatively prime. Then the system has a unique solution modulo $M = m_1 m_2 \cdots m_k$.

Consider the integer

$$x_0 = M_1 s_1 r_1 + M_2 s_2 r_2 + \cdots + M_k s_k r_k$$

where $M_i = M/m_i$ and s_i is the unique solution of $M_i x \equiv 1 \pmod{m_1}$. Let j be given. For $i \neq j$, we have $m_j | M_i$ and hence

$$M_i s_i r_i \equiv 0 \pmod{m_j}$$

On the other hand, $M_j s_j \equiv 1 \pmod{m_j}$ and hence

$$M_j s_j r_j \equiv r_j \pmod{m_j}$$

Accordingly,

$$x_0 \equiv 0 + \cdots + 0 + r_j + 0 + \cdots + 0 \equiv r_j \pmod{m_j}$$

In other words, x_0 is a solution of each of the equations in (*1*).

It remains to show that x_0 is the unique solution of the system (*1*) modulo M. Suppose x_1 is another solution of all the equations in (*1*). Then

$$x_0 \equiv x_1 \pmod{m_1}, \qquad x_0 \equiv x_1 \pmod{m_2}, \qquad \ldots, \qquad x_0 \equiv x_1 \pmod{m_k}$$

Hence $m_i | (x_0 - x_1)$, for each i. Since the m_i are relatively prime, $M = \text{lcm}(m_1, m_2, \ldots, m_k)$ and so $M | (x_0 - x_1)$. That is,

$$x_0 \equiv x_1 \pmod{M}$$

Thus the theorem is proved.

Supplementary Problems

ORDER AND INEQUALITIES, ABSOLUTE VALUE

11.69. Insert the correct symbol, $<$, $>$, or $=$, between each pair of integers:

(*a*) $2 \_\_\_\_ -6$ (*c*) $-7 \_\_\_\_ 3$ (*e*) $2^3 \_\_\_\_ 11$ (*g*) $-2 \_\_\_\_ -7$

(*b*) $-3 \_\_\_\_ -5$ (*d*) $-8 \_\_\_\_ -1$ (*f*) $2^3 \_\_\_\_ -9$ (*h*) $4 \_\_\_\_ -9$

11.70. Evaluate: (*a*) $|-6|, |5|, |0|$; (*b*) $|3-7|, |-3+7|, |-3-7|$.

11.71. Evaluate: (*a*) $|2-5| + |3+7|, |1-4| - |2-9|$; (*b*) $|-4| + |2-3|, |-6-2| - |2-6|$

11.72. Find the distance d between each pair of integers:

(*a*) 2 and -5; (*b*) -6 and 3; (*c*) 2 and 8; (*d*) -7 and -1; (*e*) 3 and -3; (*f*) -7 and -9.

11.73. Find all integers n such that: (*a*) $3 < 2n - 4 < 10$; (*b*) $1 < 6 - 3n < 13$.

11.74. Prove Proposition 11.1: (i) $a \leq a$, for any integer a; (ii) If $a \leq b$ and $b \leq a$, then $a = b$.

11.75. Prove Proposition 11.2: For any integers a and b, exactly one of the following holds: $a < b$, $a = b$, or $a > b$.

11.76. Prove: (*a*) $2ab \leq a^2 + b^2$; (*b*) $ab + ac + bc \leq a^2 + b^2 + c^2$.

11.77. Proposition 11.4: (i) $|a| \geq 0$, and $|a| = 0$ iff $a = 0$. (ii) $-|a| \leq a \leq |a|$. (v) $| \, |a| - |b| \, | \leq |a \pm b|$

11.78. Show that $a - xb \geq 0$ if $b \neq 0$, and $x = -|a|b$.

MATHEMATICAL INDUCTION, WELL-ORDERING PRINCIPLE

11.79. Prove the proposition that the sum of the first n even positive integers is $n(n + 1)$; that is,

$$P(n): \quad 2 + 4 + 6 + \cdots + 2n = n(n + 1)$$

11.80. Prove the proposition that the sum of the first n cubes is equal to the square of the sum of the first n positive integers; that is,

$$P(n): \quad 1^3 + 2^3 + 3^3 + \cdots + n^3 = (1 + 2 + \cdots + n)^2$$

11.81. Prove: $1 + 4 + 7 + \cdots + (3n - 2) = n(3n - 1)/2$.

11.82. Prove: (*a*) $a^n a^m = a^{n+m}$; (*b*) $(a^n)^m = a^{nm}$; (*c*) $(ab)^n = a^n b^n$

11.83. Prove: $\dfrac{1}{1 \cdot 2} + \dfrac{1}{2 \cdot 3} + \dfrac{1}{3 \cdot 4} + \cdots + \dfrac{1}{n(n+1)} = \dfrac{n}{n+1}$.

11.84. Prove: $\dfrac{1}{1 \cdot 3} + \dfrac{1}{3 \cdot 5} + \dfrac{1}{5 \cdot 7} + \cdots + \dfrac{1}{(2n-1)(2n+1)} = \dfrac{n}{2n+1}$.

11.85. Prove: $\dfrac{1^2}{1 \cdot 3} + \dfrac{2^2}{3 \cdot 5} + \dfrac{3^2}{5 \cdot 7} + \cdots + \dfrac{n^2}{(2n-1)(2n+1)} = \dfrac{n(n+1)}{2(2n+1)}$.

11.86. Prove:

(*a*) $x^{n+1} - y^{n+1} = (x - y)(x^n + x^{n-1}y + x^{n-2}y^2 + \cdots + y^n)$.

(*b*) $a^{n+1} + b^{n+1} = (a + b)(a^n - a^{n-1}b + a^{n-2}b^2 - \cdots - ab^{n-1} + b^n)$.

11.87. Prove: $|P(A)| = 2^n$ where $|A| = n$. [Here $P(A)$ is the power set the finite set A with n elements.]

DIVISION ALGORITHM

11.88. For each pair of integers a and b, find integers q and r such that $a = bq + r$ and $0 \leq r < |b|$:

(*a*) $a = 395$ and $b = 14$. (*c*) $a = -278$ and $b = 12$.

(*b*) $a = 608$ and $b = -17$. (*b*) $a = -417$ and $b = -8$.

11.89. Prove each of the following statements:

(*a*) Any integer a is of the form $5k$, $5k + 1$, $5k + 2$, $5k + 3$, or $5k + 4$.

(*b*) One of five consecutive integers is a multiple of 5.

11.90. Prove each of the following statements:

(*a*) The product of any three consecutive integers is divisible by 6.

(*b*) The product of any four consecutive integers is divisible by 24.

11.91. Show that each of the following numbers is not rational: (*a*) $\sqrt{3}$; (*b*) $\sqrt[3]{2}$.

11.92. Show that $\sqrt{p}$ is not rational, where p is any prime number.

DIVISIBILITY, GREATEST COMMON DIVISORS, PRIMES

11.93. Find all possible divisors of: (*a*) 24; (*b*) $19683 = 3^9$; (*c*) $432 = 2^4 \cdot 3^3$.

11.94. List all prime numbers between 100 and 150.

11.95. Express as a product of prime numbers: (*a*) 2940; (*b*) 1485; (*c*) 8712; (*d*) 319 410.

11.96. For each pair of integers a and b, find $d = \gcd(a, b)$ and express d as a linear combination of a and b:

(*a*) $a = 48$, $b = 356$. (*c*) $a = 2310$, $b = 168$.

(*b*) $a = 165$, $b = 1287$. (*d*) $a = 195$, $b = 968$.

11.97. Find: (*a*) $\text{lcm}(5, 7)$; (*b*) $\text{lcm}(3, 33)$; (*c*) $\text{lcm}(12, 28)$.

11.98. Suppose $a = 5880$ and $b = 8316$.

(*a*) Express a and b as products of primes

(*b*) Find $\gcd(a, b)$ and $\text{lcm}(a, b)$.

(*c*) Verify that $\text{lcm}(a, b) = (|ab|)/\gcd(a, b)$.

11.99. Prove: (*a*) If $a|b$, then $a| - b$, $-a|b$, and $-a| - b$. (*b*) If $ac|bc$, then $b|c$.

11.100. Prove:

(*a*) If $n > 1$ is composite, then n has a positive divisor d such that $d \leq \sqrt{n}$.

(*b*) If $n > 1$ is not divisible by a prime $p \leq \sqrt{n}$, then n is a prime.

11.101. Prove: (*a*) If $am + bn = 1$, then $\gcd(a, b) = 1$. (*b*) If $a = bq + r$, then $\gcd(a, b) = \gcd(b, r)$.

11.102. Prove: (*a*) $\gcd(a, a + k)$ divides k. (*b*) $\gcd(a, a + 2)$ equals 1 or 2.

11.103. Prove:

(*a*) If $a > 2$ and $k > 1$, then $a^k - 1$ is composite.

(*b*) If $n > 0$ and $2^n - 1$ is prime, then n is prime.

11.104. Let n be a positive integer. Prove:

(*a*) 3 divides n if and only if 3 divides the sum of the digits of n.

(*b*) 9 divides n if and only if 9 divides the sum of the digits of n.

(*c*) 8 divides n if and only if 8 divides the integer formed by the last three digits of n.

11.105. Extend the definition of gcd and lcm to any finite set of integers, that is, for integers $a_1, a_2, \ldots, a_k$, define:

(*a*) $\gcd(a_1, a_2, \ldots, a_k)$; (*b*) $\text{lcm}(a_1, a_2, \ldots, a_k)$.

11.106. Prove: If $a_1|n$ and $a_2|n, \ldots, a_k|n$, then $m|n$ where $m = \text{lcm}(a_1, \ldots a_k)$.

11.107. Prove: There are arbitrarily large gaps between prime numbers, that is, for any positive integer k, there exist k consecutive composite (nonprime) integers.

CONGRUENCES

11.108. Which of the following are true?

(*a*) $224 \equiv 762 \pmod 8$. (*c*) $156 \equiv -369 \pmod 7$.

(*b*) $582 \equiv 263 \pmod{11}$. (*d*) $-238 \equiv 483 \pmod{13}$.

11.109. Find the smallest nonnegative integer which is congruent modulo $m = 9$ to each of the following numbers:

(*a*) 457; (*b*) 1578; (*c*) -366; (*d*) -3288.

[The integer should be in the set $\{0, 1, 2, \ldots, 7, 8\}$.]

11.110. Find the smallest integer in absolute value which is congruent modulo $m = 9$ to each of the following numbers:

(*a*) 511; (*b*) 1329; (*c*) -625; (*d*) -2717.

[The integer should be in the set $\{-4, -3, -2, -1, 0, 1, 2, 3, 4\}$.]

11.111. Find all numbers between 1 and 100 which are congruent to 4 modulo $m = 11$.

11.112. Find all numbers between -50 and 50 which are congruent to 12 modulo $m = 9$.

RESIDUE SYSTEMS, EULER PHI FUNCTION f

11.113. For each modulo m, exhibit two complete residue systems, one consisting of the smallest nonnegative integers, and the other consisting of the integers with the smallest absolute values: (*a*) $m = 11$; (*b*) $m = 14$.

11.114. Exhibit a reduced residue system modulo m and find $\phi(m)$ where: (*a*) $m = 4$; (*b*) $m = 11$; (*c*) $m = 14$; (*d*) $m = 15$.

11.115. Exhibit a complete residue system modulo $m = 8$ consisting entirely of: (*a*) multiples of 5; (*b*) powers of 3.

11.116. Show that $\{1^2, 2^2, 3^2, \ldots, m^2\}$ is not a complete residue system modulo m for $m > 2$.

11.117. Find: (*a*) $\phi(10)$; (*b*) $\phi(12)$; (*c*) $\phi(15)$.

11.118. Find: (*a*) $\phi(3^7)$; (*b*) $\phi(5^6)$; (*c*) $\phi(2^4 \cdot 7^6 \cdot 13^3)$.

11.119. Find the number s of positive integers less than 3200 which are coprime to 800.

ARITHMETIC MODULO m, $\mathbf{Z}_m$

11.120. Exhibit the addition and multiplication tables for: (*a*) $\mathbf{Z}_2$; (*b*) $\mathbf{Z}_8$.

11.121. In $\mathbf{Z}_{13}$, find: (*a*) $-2, -3, -5, -9, -10, -11$; (*b*) 2/9, 4/9, 5/9, 7/9, 8/9.

11.122. In $\mathbf{Z}_{17}$, find: (*a*) $-3, -5, -6, -8, -13, -15, -16$; (*b*) 3/8, 5/8, 7/8, 13/8, 15/8.

11.123. Find a^{-1} in $\mathbf{Z}_m$ where: (*a*) $a = 15$, $m = 127$; (*b*) $a = 61$, $m = 124$; (*c*) $a = 12$, $m = 111$.

11.124. Find the product $f(x)g(x)$ for the following polynomials over $\mathbf{Z}_5$: $f(x) = 4x^3 - 2x^2 + 3x - 1$, $g(x) = 3x^2 - x - 4$

CONGRUENCE EQUATIONS

11.125. Solve each congruence equation:

(*a*) $f(x) = 2x^3 - x^2 + 3x + 1 \equiv 0 \pmod 5$.

(*b*) $g(x) = 3x^4 - 2x^3 + 5x^2 + x + 2 \equiv 0 \pmod 7$.

(*c*) $h(x) = 45x^3 - 37x^2 + 26x + 312 \equiv 0 \pmod 6$.

11.126. Solve each linear congruence equation:

(*a*) $7x \equiv 3 \pmod 9$; (*b*) $4x \equiv 6 \pmod{14}$; (*c*) $6x \equiv 4 \pmod 9$.

11.127. Solve each linear congruence equation:

(*a*) $5x \equiv 3 \pmod 8$; (*b*) $6x \equiv 9 \pmod{16}$; (*c*) $9x \equiv 12 \pmod{21}$.

11.128. Solve each linear congruence equation:

(*a*) $37x \equiv 1 \pmod{249}$; (*b*) $195 \equiv 23 \pmod{968}$.

11.129. Solve each linear congruence equation:

(*a*) $132x \equiv 169 \pmod{735}$; (*b*) $48 \equiv 284 \pmod{356}$.

11.130. A puppet theater has only 60 seats. The admission to the theater is \$2.25 per adult and \$1.00 per child. Suppose \$117.25 was collected. Find the number of adults and children attending the performance.

11.131. Find the smallest positive solution of each system of congruence equations:

(*a*) $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$, $x \equiv 4 \pmod{11}$.

(*b*) $x \equiv 3 \pmod 5$, $x \equiv 4 \pmod 7$; $x \equiv 6 \pmod 9$.

11.132. Find the smallest positive solution of the following system of congruence equations:

$$x \equiv 5 \pmod{45}; \qquad x \equiv 6 \pmod{49}; \qquad x \equiv 7 \pmod{52}$$

Answers to Supplementary Problems

11.69. (*a*) $2 > -6$; (*b*) $-3 > -5$; (*c*) $-7 < 3$; (*d*) $-8 < -1$, (*e*) $2^3 < 11$; (*f*) $2^3 > -9$; (*g*) $-2 > -7$; (*h*) $4 > -9$.

11.70. (*a*) 6, 5, 0; (*b*) 4, 4, 10.

11.71. (*a*) $3 + 10 = 13$, $3 - 7 = -4$; (*b*) $4 + 1 = 5$, $8 - 4 = 4$.

11.72. (*a*) 7; (*b*) 9; (*c*) 6; (*d*) 6; (*e*) 6; (*f*) 3.

11.73. (*a*) 4, 5, 6; (*b*) $-2, -1, 0, 1$.

11.88. (*a*) $q = 28$, $r = 3$; (*b*) $q = -15$, $r = 13$; (*c*) $q = -24$, $r = 10$; (*d*) $q = 53$, $r = 7$.

11.90. (*a*) One is divisible by 2 and one is divisible by 3.
(*b*) One is divisible by 4, another is divisible by 2, and one is divisible by 3.

11.93. (*a*) 1, 2, 3, 4, 6, 12, 24; (*b*) 3^n for $n = 0$ to 9; (*c*) $2^r 3^s$ for $r = 0$ to 4 and $s = 0$ to 3.

11.94. 101, 103, 107, 109, 113, 127, 131, 137, 139, 149.

11.95. (*a*) $2940 = 2^2 \cdot 3 \cdot 5 \cdot 7^2$; (*b*) $1485 = 3^3 \cdot 5 \cdot 11$; (*c*) $8712 = 2^3 \cdot 3^2 \cdot 11^2$; (*d*) $319\,410 = 2 \cdot 3^3 \cdot 5 \cdot 7 \cdot 13^2$.

11.96. (*a*) $d = 4 = 5(356) - 37(48)$; (*b*) $d = 33 = 8(165) - 1(1287)$; (*c*) $d = 42 = 14(168) - 1(2310)$; (*d*) $d = 1 = 139(195) - 28(968)$.

11.97. (*a*) 35; (*b*) 33; (*c*) 84.

11.98. (*a*) $a = 2^4 \cdot 3 \cdot 5 \cdot 7^2$, $b = 2^2 \cdot 3^3 \cdot 7 \cdot 11$.
(*b*) $\gcd(a, b) = 2^2 \cdot 3 \cdot 7$, $\text{lcm}(a, b) = 2^4 \cdot 3^3 \cdot 5 \cdot 7^2 \cdot 11 = 1\,164\,240$.

11.103. (*a*) *Hint*: $a^k - 1 = (a - 1)(1 + a + a^2 + \cdots + a^{k-1})$.
(*b*) *Hint*: If $n = ab$, then $2^n - 1 = (2^a)^b - 1$.

11.107. $(k + 1)! + 2$, $(k + 1)! + 3$, $(k + 1)! + 4, \ldots,$ $(k + 1)! + (k + 1)$ are divisible by 2, 3, 4, $\ldots, k + 1$, respectively.

11.108. (*a*) False; (*b*) true; (*c*) true; (*d*) false.

11.109. (*a*) 7; (*b*) 2; (*c*) 3; (*d*) 6.

11.110. (*a*) -2; (*b*) -3; (*c*) -2; (*d*) 1.

11.111. 4, 15, 26, 37, 48, 59, 70, 81, 92.

11.112. $-42, -33, -24, -15, -6, 3, 12, 21, 30, 39, 48$.

11.113. (*a*) $\{0, 1, \ldots, 10\}$ and $\{-5, -4, \ldots, -1, 0, 1, \ldots 4, 5\}$.
(*b*) $\{0, 1, \ldots, 13\}$ and $\{-6, -5, \ldots, -1, 0, 1, \ldots, 6, 7\}$.

11.114. (*a*) $\{1,3\}$; (*b*) $\{1,2,\ldots,10\}$; (*c*) $\{1,3,5,9,11,13\}$; (*d*) $\{1,2,4,7,8,11,13,14\}$.

11.115. (*a*) $\{5,10,15,20,25,30,35,40\}$; (*b*) $\{3,9,27,81,243,729,2187,6561\}$.

11.116. $m-1 \equiv -1 \pmod{m}$ and so $(m-1)^2 \equiv (-1)^2 = 1^2 \pmod{m}$.

11.117. (*a*) $\phi(10) = 4$; (*b*) $\phi(12) = 4$; (*c*) $\phi(15) = 8$.

11.118. (*a*) $\phi(3^7) = 2 \cdot 3^6$; (*b*) $\phi(5^6) = 4 \cdot 5^5$; (*c*) $\phi(2^4 \cdot 7^6 \cdot 13^3) = (2^3)(6 \cdot 7^5)(12 \cdot 13^2)$.

11.119. $\phi(8000) = \phi(2^5 \cdot 5^2) = 2^4 \cdot 4 \cdot 5 = 320$. Hence $s = 4(320) = 1280$.

11.121. (*a*) $-2 = 11$, $-3 = 10$, $-5 = 8$, $-9 = 4$, $-10 = 3$, $-11 = 2$,
(*b*) (*Hint*: First compute the multiplication table for 9 modulo 13.)
$2/9 = 6, 4/9 = 12, 5/9 = 2, 7/9 = 8, 8/9 = 11$.

11.122. (*a*) $-3 = 14$, $-5 = 12$, $-6 = 11$, $-8 = 9$, $-13 = 4$, $-15 = 2$.
(*b*) $3/8 = 11$, $5/8 = 7$, $7/8 = 3$, $13/8 = 8$, $15/8 = 4$.

11.123. (*a*) $a^{-1} = 17$; (*b*) $a^{-1} = 61$; (*c*) a^{-1} does not exist.

11.124. $f(x)g(x) = 2x^5 + 2x^2 - x + 4$.

11.125. (*a*) 1, 3, 4; (*b*) 2, −2; (*c*) 0, 2, 3, −1.

11.126. (*a*) 3; (*b*) 5, 12; (*c*) no solution.

11.127. (*a*) 7; (*b*) no solution; (*c*) 6, 13, 20.

11.128. (*a*) 175; (*b*) 293.

11.129. (*a*) No solution; (*b*) 43, 132, 221, 310.

11.130. 12 adults and 47 children, or 3 adults and 51 children.

11.131. (*a*) 158; (*b*) 123.

11.132. 31 415.

© The McGraw–Hill Companies, 2004

Chapter 12

Algebraic Systems

12.1 INTRODUCTION

This section investigates some of the major algebraic systems in mathematics: semigroups, groups, rings, and fields. We also define the notion of a homomorphism and the notion of a quotient structure. We begin with the formal definition of an operation, and discuss various types of operations.

12.2 OPERATIONS

The reader is familiar with the operations of addition and multiplication of numbers, union and intersection of sets, and the composition of functions. These operations are denoted as follows:

$$a + b = c, \qquad a \cdot b = c, \qquad A \cup B = C, \qquad A \cap B = C, \qquad g \circ f = h.$$

In each situation, an element (c, C, or h) is assigned to an original pair of elements. In other words, there is a function which assigns a unique element to any given pair of elements. We now make this notion precise.

Definition: Let S be a nonempty set. An *operation* on S is a function $*$ from $S \times S$ into S. In such a case, we usually write

$$a * b \qquad \text{or sometimes} \qquad ab$$

instead of $*(a, b)$. The set S and an operation $*$ on S is denoted by $(S, *)$ or simply S when the operation is understood.

Remark: An operation $*$ from $S \times S$ into S is sometimes called a *binary* operation. A *unary* operation is a function from S into S. For example, the absolute value $|n|$ of an integer n is a unary operation on $\mathbf{Z}$, and the complement A^c of a set A is a unary operation on the power set $P(X)$ of a set X. A *ternary* (3-ary) operation is a function from $S \times S \times S$ into S. More generally, an *n-ary* operation is a function from $S \times S \times \cdots \times S$ (n factors) into S. Unless otherwise stated, the word operation shall mean binary operation. We will also assume that our underlying set S is nonempty.

Suppose S is a finite set. Then an operation $*$ on S can be presented by its operation (multiplication) table where the entry in the row labeled a and the column labeled b is $a * b$.

Suppose S is a set with an operation $*$, and suppose A is a subset of S. Then A is said to be *closed under* $*$ if $a * b$ belongs to A for any elements a and b in A.

EXAMPLE 12.1 Consider the set $\mathbf{N}$ of positive integers.

(a) Addition ($+$) and multiplication ($\times$) are operations on $\mathbf{N}$. However, subtraction ($-$) and division ($/$) are not operations on $\mathbf{N}$ since the difference and the quotient of positive integers need not be positive integers. For example, $2 - 9$ and $7/3$ are not positive integers.

(b) Let A and B denote, respectively, the set of even and odd positive integers. Then A is closed under addition and multiplication since the sum and product of any even numbers are even. On the other hand, B is closed under multiplication but not addition since, for example, $3 + 5 = 8$ is even.

EXAMPLE 12.2

(a) Let $S = \{0, 1, -1\}$. Then addition $+$ is not an operation on S since the sum $1 + 1$ is not an element of S. On the other hand, multiplication is an operation on S.

(*b*) Let S denote the collection of all integer 2×2 matrices:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

Then matrix addition and matrix multiplication are operations on S. Let A and B be the subsets of S consisting, respectively, of all matrices of the form

$$\begin{bmatrix} a & b \\ c & 0 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$$

Then A is closed under matrix addition but not matrix multiplication, e.g.,

$$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \quad \begin{bmatrix} 1 & 2 \\ 3 & 0 \end{bmatrix} = \begin{bmatrix} 4 & 2 \\ 1 & 2 \end{bmatrix}$$

On the other hand, B is closed under the operations of matrix addition and matrix multiplication.

EXAMPLE 12.3 Let $S = \{a, b, c, d\}$. The tables in Fig. 12-1 define operations $*$ and $\cdot$ on S. Note that $*$ can be defined by the formula

$$x * y = x$$

where x and y are any elements of S.

$*$	a	b	c	d
a	a	a	a	a
b	b	b	b	b
c	c	c	c	c
d	d	d	d	d

(*a*)

$\cdot$	a	b	c	d
a	a	b	c	d
b	b	a	a	b
c	c	b	a	a
d	d	a	a	a

(*b*)

Fig. 12-1

Properties of Operations

This subsection lists a number of important properties of our operations.

(1) **Associative and Commutative Laws:**

An operation $*$ on a set S is said to be *associative* or to satisfy the *associative law* if, for any elements a, b, c in S, we have

$$(a * b) * c = a * (b * c)$$

Generally speaking, if an operation is not associative, then there may be many ways to form a product. For example, the following shows five ways to form the product abcd:

$$((ab)c)d, \quad (ab)(cd), \quad (a(bc))d, \quad a((bc)d), \quad a(b(cd))$$

If the operation is associative, then the following theorem (proved in Problem 12.7) applies.

Theorem 12.1: Suppose $*$ is an associative operation on a set S. Then any product $a_1 * a_2 * \cdots * a_n$ requires no parenthesis, that is, all possible products are equal.

An operation $*$ on a set S is said to be *commutative* or satisfy the *commutative law* if

$$a * b = b * a$$

for any elements a, b in S.

EXAMPLE 12.4

(*a*) Consider the set $\mathbf{Z}$ of integers. Addition and multiplication of integers are associative and commutative. On the other hand, subtraction is nonassociative. For example,

$$(8 - 4) - 3 = 1 \qquad \text{but} \qquad 8 - (4 - 3) = 7$$

Moreover, subtraction is noncommutative since, for example, $3 - 7 \neq 7 - 3$.

(*b*) Consider the operation of matrix multiplication on the set M of n-square matrices. One can prove (Section 5.5) that matrix multiplication is associative. On the other hand, matrix multiplication is noncommutative. For example,

$$\begin{bmatrix}1 & 2\\ 3 & 4\end{bmatrix}\begin{bmatrix}5 & 6\\ 0 & -2\end{bmatrix} = \begin{bmatrix}5 & 2\\ 15 & 10\end{bmatrix} \qquad \text{but} \qquad \begin{bmatrix}5 & 6\\ 0 & -2\end{bmatrix}\begin{bmatrix}1 & 2\\ 3 & 4\end{bmatrix} = \begin{bmatrix}23 & 34\\ -6 & -8\end{bmatrix}$$

(*c*) Consider the exponential operation $a * b = a^b$ on the set $\mathbf{N}$ of positive integers. The operation is nonassociative. For example,

$$(2 * 2) * 3 = (2^2)^3 = 4^3 = 64 \qquad \text{but} \qquad 2 * (2 * 3) = 2^{2^3} = 2^8 = 256$$

Moreover, $*$ in noncommutative. For example,

$$2 * 3 = 2^3 = 8 \qquad \text{but} \qquad 3 * 2 = 3^2 = 9$$

(*d*) Consider the operation on $S = \{a, b, c, d\}$ defined by the table in Fig. 12-1(*b*). The operation is nonassociative. For example,

$$(b \cdot c) \cdot c = a \cdot c = c \qquad \text{but} \qquad b \cdot (c \cdot c) = b \cdot a = b$$

Moreover, the operation is noncommutative. For example, $b \cdot c = a$ but $c \cdot b = b$.

(2) **Identity Element and Inverses:**

Consider an operation $*$ on a set S. An element e in S is called an *identity* element for $*$ if, for any element a in S,

$$a * e = e * a = a$$

More generally, an element e is called a *left identity* or a *right identity* according as $e * a = a$ or $a * e = a$ where a is any element in S. The following theorem applies.

Theorem 12.2: Suppose e is a left identity and f is a right identity for an operation on a set S. Then $e = f$.

The proof is very simple. Since e is a left identity, $ef = f$; but since f is a right identity, $ef = e$. Thus $e = f$. This theorem tells us, in particular, that an identity element is unique, and that if an operation has more than one left identity then it has no right identity, and vice versa.

Suppose an operation $*$ on a set S does have an identity element e. The *inverse* of an element a in S is an element b such that

$$a * b = b * a = e$$

If the operation is associative, then the inverse of a, if it exists, is unique (Problem 12.3). Observe that if b is the inverse of a, then a is the inverse of b. Thus the inverse is a symmetric relation, and we can say that the elements a and b are inverses.

Notation: If the operation on S is denoted by $a * b$, $a \times b$, $a \cdot b$ or ab, then S is said to be written *multiplicatively* and the inverse of an element a in S is usually denoted by a^{-1}. Sometimes, when S is commutative, the operation is denoted by $+$ and then S is said to be written *additively*. In such a case, the identity element is usually denoted by 0 and is called the *zero* element; and the inverse is denoted by $-a$ and is called the *negative* of a.

EXAMPLE 12.5

(*a*) Consider the rational numbers $\mathbf{Q}$. Under addition, 0 is the identity element, and -3 and 3 are (additive) inverses since

$$(-3) + 3 = 3 + (-3) = 0$$

On the other hand, under multiplication, 1 is the identity element, and -3 and $-\frac{1}{3}$ are (multiplicative) inverses since

$$(-3) \cdot \left(-\frac{1}{3}\right) = \left(-\frac{1}{3}\right) \cdot (-3) = 1$$

Note 0 has no multiplicative inverse.

(*b*) Consider the set $S = \{a, b, c, d\}$ under the operation defined by Fig. 12-1(*b*). Note that the element a is an identity element. Also, note that $dd = a$, so d is its own inverse. Furthermore, $dc = cd = a$ and so c and d are also inverses. Thus the inverse of d is not unique. (This means that the operation cannot be associative.)

(3) **Cancelation Laws:**

An operation $*$ on a set S is said to satisfy the *left cancelation law* if

$$a * b = a * c \text{ implies } b = c$$

and is said to satisfy the *right cancelation law* if

$$b * a = c * a \text{ implies } b = c$$

Addition and subtraction of integers in **Z** and multiplication of nonzero integers in **Z** do satisfy both the left and right cancelation laws. On the other hand, matrix multiplication does not satisfy the cancelation laws. For example, suppose

$$A = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}, \qquad B = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \qquad C = \begin{bmatrix} 0 & -3 \\ 1 & 5 \end{bmatrix}, \qquad D = \begin{bmatrix} 1 & 2 \\ 0 & 0 \end{bmatrix}$$

Then $AB = AC = D$, but $B \neq C$.

12.3 SEMIGROUPS

Let S be a nonempty set with an operation. Then S is called a *semigroup* if the operation is associative. If the operation also has an identity element, then S is called a *monoid*.

EXAMPLE 12.6

(*a*) Consider the positive integers **N**. Then $(\mathbf{N}, +)$ and $(\mathbf{N}, \times)$ are semigroups since addition and multiplication on **N** are associative. In particular, $(\mathbf{N}, \times)$ is a monoid since it has the identity element 1. However, $(\mathbf{N}, +)$ is not a monoid since addition in **N** has no zero element.

(*b*) Let S be a finite set, and let $F(S)$ be the collection of all functions $f: S \to S$ under the operation of composition of functions. Since the composition of functions is associative, $F(S)$ is a semigroup. In fact, $F(S)$ is a monoid since the identity function is an identity element for $F(S)$.

(*c*) Let $S = \{a, b, c, d\}$. The multiplication tables in Fig. 12-1 define operations $*$ and $\cdot$ on S. Note that $*$ can be defined by the formula $x * y = x$ for any x and y in S. Hence

$$(x * y) * z = x * z = x \qquad \text{and} \qquad x * (y * z) = x * y = x$$

Therefore, $*$ is associative and hence $(S, *)$ is a semigroup. On the other hand, $\cdot$ is not associative since, for example,

$$(b \cdot c) \cdot c = a \cdot c = c \qquad \text{but} \qquad b \cdot (c \cdot c) = b \cdot a = b$$

Thus $(S, \cdot)$ is not a semigroup.

Free Semigroup, Free Monoid

Let A be a nonempty set. A *word* w on A is a finite sequence of its elements. For example,

$$u = ababbbb = abab^4 \qquad \text{and} \qquad v = baccaaaa = bac^2a^4$$

are words on $A = \{a, b, c\}$. (We write a^2 for aa, a^3 for aaa, and so on.) The length of a word w, denoted by l(w), is the number of elements in w. Thus $l(u) = 7$ and $l(v) = 8$.

The *concatenation* of words u and v on a set A, written $u * v$ or uv, is the word obtained by writing down the elements of u followed by the elements of v. For example,

$$uv = (abab^4)(bac^2a^4) = abab^5c^2a^4$$

Now let $F = F(A)$ denote the collection of all words on A under the operation of concatenation. Clearly, for any words u, v, w, the words $(uv)w$ and $u(vw)$ are identical; they simply consist of the elements of u, v, w written down one after the other. Thus F is a semigroup; it is called the *free semigroup* on A, and the elements of A are called the *generators* of F.

The empty sequence, denoted by λ, is also considered as a word on A. However, we do not assume that λ belongs to the free semigroup $F = F(A)$. The set of all words on A including λ is frequently denoted by A^*. Thus A^* is a monoid under concatenation; it is called the free monoid on A.

Subsemigroups

Let A be a nonempty subset of a semigroup S. Then A is called a *subsemigroup* of S if A itself is a semigroup with respect to the operation on S. Since the elements of A are also elements of S, the associative law automatically holds for the elements of A. Therefore, A is a subsemigroup of S if and only if A is closed under the operation on S.

EXAMPLE 12.7

(*a*) Let A and B denote, respectively, the set of even and odd positive integers. Then $(A, \times)$ and $(B, \times)$ are subsemigroups of $(\mathbf{N}, \times)$ since A and B are closed under multiplication. On the other hand, $(A, +)$ is a subsemigroup of $(\mathbf{N}, +)$ since A is closed under addition, but $(B, +)$ is not a subsemigroup of $(\mathbf{N}, +)$ since B is not closed under addition.

(*b*) Consider the free semigroup F on the set $A = \{a, b\}$. Let H consist of all *even* words, that is, words with even length. The concatenation of two such words is also even. Thus H is a subsemigroup of F.

Congruence Relations and Quotient Structures

Let S be a semigroup and let $\sim$ be an equivalence relation on S. Recall that the equivalence relation $\sim$ induces a partition of S into equivalence classes where $[a]$ denotes the equivalence class containing the element a in S, and that the collection of equivalence classes is denoted by $S/\sim$.

Suppose that the equivalence relation $\sim$ on S has the following property:

$$\text{If } a \sim a' \text{ and } b \sim b', \text{ then } ab \sim a'b'.$$

Then $\sim$ is called a *congruence relation* on S. Furthermore, we can now define an operation on the equivalence classes by

$$[a] * [b] = [a * b] \qquad \text{or, simply,} \qquad [a][b] = [ab]$$

Furthermore, this operation on $S/\sim$ is associative; hence $S/\sim$ is a semigroup. We state this result formally.

Theorem 12.3: Let $\sim$ be a congruence relation on a semigroup S. Then $S/\sim$, the equivalence classes under $\sim$, form a semigroup under the operation

$$[a][b] = [ab]$$

This semigroup $S/\sim$ is called the *quotient* of S by $\sim$.

EXAMPLE 12.8

(*a*) Let F be the free semigroup on a set A. Define $u \sim u'$ if u and u' have the same length. Then $\sim$ is an equivalence relation on F. Furthermore, suppose $u \sim u'$ and $v \sim v'$, say,

$$\ell(u) = \ell(u') = m \qquad \text{and} \qquad \ell(v) = \ell(v') = n$$

Then $\ell(uv) = \ell(u'v') = m + n$, and so $uv \sim u'v'$. Thus $\sim$ is a congruence relation on F.

(*b*) Consider the integers $\mathbf{Z}$ and a positive integer $m > 1$. Recall (Section 11.8) that we say that a is *congruent to b modulo m*, written

$$a \equiv b \pmod{m}$$

if m divides the difference $a - b$. Theorem 11.20 states that this relation is an equivalence relation on $\mathbf{Z}$.

Furthermore, Theorem 11.21 tells us that if $a \equiv c \pmod{m}$ and $b \equiv d \pmod{m}$ then

$$a + b \equiv c + d \pmod{m} \qquad \text{and} \qquad ab \equiv cd \pmod{m}$$

In other words, this relation is a congruence relation on Z.

Homomorphism of Semigroups

Consider two semigroups $(S, *)$ and $(S', *')$. A function $f: S \to S'$ is called a *semigroup homomorphism* or, simply, a *homomorphism* if

$$f(a * b) = f(a) *' f(b) \qquad \text{or, simply} \qquad f(ab) = f(a)f(b).$$

Suppose f is also one-to-one and onto. Then f is called an *isomorphism* between S and S'; and S and S' are said to be *isomorphic* semigroups, written $S \approx S'$.

EXAMPLE 12.9

(*a*) Let F be the free semigroup on a set A, and let $\mathbf{Z}$ denote the integers under addition. Suppose

$$f: F \to \mathbf{Z} \qquad \text{is defined by} \qquad f(w) = \ell(w)$$

Then f is a homomorphism since $\ell(uv) = \ell(u) + \ell(v)$. That is, for any words u, v in F,

$$f(uv) = \ell(uv) = \ell(u) + \ell(v) = f(u) + f(v)$$

Observe that the operation in F is written multiplicatively, whereas the operation in $\mathbf{Z}$ is addition.

(*b*) Figure 12-2(*a*) gives the addition table for $\mathbf{Z}_4$, the integers modulo 4 under addition; and Fig. 12-2(*b*) gives the multiplication table for $S = \{1, 3, 7, 9\}$ in $\mathbf{Z}_{10}$. (We note that S is a reduced residue system for the integers $\mathbf{Z}$ modulo 10.) Let $f: \mathbf{Z}_4 \to S$ be defined by

$$f(0) = 1, \qquad f(1) = 3, \qquad f(2) = 9, \qquad f(3) = 7$$

One can show that f is a homomorphism. Since f is also one-to-one and onto, f is an isomorphism. Thus $\mathbf{Z}_4$ and S are isomorphic semigroups.

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

(*a*)

×	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

(*b*)

Fig. 12-2

(*c*) Let M be the set of all 2×2 matrices with integer entries. The determinant of any matrix $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is denoted and defined by $\det(A) = |A| = ad - bc$. One proves in Linear Algebra that the determinant is a multiplicative function, that is, for any matrices A and B,

$$\det(AB) = \det(A) \cdot \det(B)$$

Thus the determinant function is a semigroup homomorphism on $(M, \times)$, the matrices under matrix multiplication. On the other hand, the determinant function is not additive, that is, for some matrices,

$$\det(A + B) \neq \det(A) + \det(B)$$

Thus the determinant function is not a semigroup homomorphism on $(M, +)$.

(*d*) Let $\sim$ be a congruence relation on a semigroup S. Let ϕ: $S \to S/\sim$ be the *natural mapping* from S into the factor semigroup $S/\sim$ defined by

$$\phi(a) = [a]$$

That is, each element a in S is assigned its equivalence class $[a]$. Then ϕ is a homomorphism since

$$\phi(ab) = [ab] = [a][b] = \phi(a)\phi(b)$$

Fundamental Theorem of Semigroup Homomorphisms

Recall that the image of a function $f: S \to S'$, written $f(S)$ or $\mathrm{Im} f$, consists of the images of the elements of S under f; that is,

$$\mathrm{Im} f = \{b \in S' : \text{there exists } a \in S \text{ for which } f(a) = b\}$$

The following theorem (proved in Problem 12.8) is fundamental to semigroup theory.

Theorem 12.4: Let $f: S \to S'$ be a semigroup homomorphism. Let $a \sim b$ if $f(a) = f(b)$. Then:
(i) $\sim$ is a congruence relation on S.
(ii) $S/\sim$ is isomorphic to $f(S)$.

EXAMPLE 12.10

(*a*) Let F be the free semigroup on $A = \{a, b\}$. The function $f: F \to \mathbf{Z}$ defined by

$$f(u) = \ell(u)$$

is a homomorphism. Note $f(F) = \mathbf{N}$. Thus $F/\sim$ is isomorphic to $\mathbf{N}$.

(*b*) Let M be the set of 2×2 matrices with integer entries. Consider the determinant function det: $M \to \mathbf{Z}$. For any integer a, we have

$$\det\begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix} = a$$

Thus the image of det is $\mathbf{Z}$. By Theorem 12.4, $M/\sim$ is isomorphic to Z.

Semigroup Products

Let $(S_1, *_1)$ and $(S_2, *_2)$ be semigroups. We form a new semigroup $S = S_1 \otimes S_2$, called the *direct product* of S_1 and S_2, as follows.

(1) The elements of S come from $S_1 \times S_2$, that is, the elements of S are ordered pairs (a, b) where $a \in S_1$ and $b \in S_2$.
(2) The operation $*$ in S is defined componentwise, that is,

$$(a, b) * (a', b') = (a *_1 a', b *_2 b') \qquad \text{or simply} \qquad (a, b)(a', b') = (aa', bb')$$

One can easily show (e.g., as in Problem 12.5(*a*)) that the above operation is associative.

12.4 GROUPS

Let G be a nonempty set with a binary operation (denoted by juxtaposition). Then G is called a *group* if the following axioms hold:

$[\mathbf{G}_1]$ *Associative law:* For any a, b, c in G, we have $(ab)c = a(bc)$.

$[\mathbf{G}_2]$ *Identity element*: There exists an element e in G such that $ae = ea = a$ for every a in G.

$[\mathbf{G}_3]$ *Inverses*: For each a in G, there exists an element a^{-1} in G (the *inverse* of a) such that

$$aa^{-1} = a^{-1}a = e$$

A group G is said to be *abelian* (or *commutative*) if the *commutative law* holds, i.e., if $ab = ba$ for every $a, b \in G$.

When the binary operation is denoted by juxtaposition as above, the group G is said to be written *multiplicatively*. Sometimes, when G is abelian, the binary operation is denoted by $+$ and G is said to be written *additively*. In such a case the identity element is denoted by 0 and is called the *zero* element; and the inverse is denoted by $-a$ and it is called the *negative* of a.

The number of elements in a group G, denoted by $|G|$, is called the *order* of G, and G is called a *finite group* if its order is finite. If A and B are subsets of G then we write

$$AB = \{ab : a \in A, b \in B\} \qquad \text{or} \qquad A + B = \{a + b : a \in A, b \in B\}$$

EXAMPLE 12.11

(*a*) The set $\mathbf{Z}$ of integers is an abelian group under addition. The identity element is 0 and $-a$ is the additive inverse of a in $\mathbf{Z}$.

(*b*) The nonzero rational numbers $Q\backslash\{0\}$ form an abelian group under multiplication. The number 1 is the identity element and q/p is the multiplicative inverse of the rational number p/q.

(*c*) Let S be the set of 2×2 matrices with rational entries under the operation of matrix multiplication. Then S is not a group since inverses do not always exist. However, let G be the subset of 2×2 matrices with a nonzero determinant. Then G is a group under matrix multiplication. The identity element is

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ and the inverse of } A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ is } A^{-1} = \begin{pmatrix} d/|A| & -b/|A| \\ -c/|A| & a/|A| \end{pmatrix}.$$

This is an example of a nonabelian group since matrix multiplication is noncommutative.

(*d*) Recall that $\mathbf{Z}_m$ denotes the integers modulo m. $\mathbf{Z}_m$ is a group under addition, but it is not a group under multiplication. However, let $\mathbf{U}_m$ denote a reduced residue system modulo m which consists of those integers relatively prime to m. Then $\mathbf{U}_m$ is a group under multiplication (modulo m). For example, Fig. 12-3 gives the multiplication table for $\mathbf{U}_{12} = \{1, 5, 7, 11\}$.

$\times$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

Fig. 12-3

	ϵ	σ_1	σ_2	σ_3	ϕ_1	ϕ_2
ϵ	ϵ	σ_1	σ_2	σ_3	ϕ_1	ϕ_2
σ_1	σ_1	ϵ	ϕ_1	ϕ_2	σ_2	σ_3
σ_2	σ_2	ϕ_2	ϵ	ϕ_1	σ_3	σ_1
σ_3	σ_3	ϕ_1	ϕ_2	ϵ	σ_1	σ_2
ϕ_1	ϕ_1	σ_3	σ_1	σ_2	ϕ_2	ϵ
ϕ_2	ϕ_2	σ_2	σ_3	σ_1	ϵ	ϕ_1

Fig. 12-4

Symmetric Group S_n

A one-to-one mapping σ of the set $\{1, 2, \ldots, n\}$ onto itself is called a *permutation*. Such a permutation is denoted by

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ j_1 & j_2 & j_3 & \ldots & j_n \end{pmatrix}$$

where $j_i = \sigma(i)$.

The set of all such permutations is denoted by S_n, and there are $n! = 1 \cdot 2 \cdot \cdots \cdot n$ of them. The composition and inverses of permutations in S_n belong to S_n, and the identity function ϵ belongs to S_n. Thus S_n forms a group under composition of functions called the *symmetric group of degree n*.

The symmetric group S_3 has $3! = 6$ elements as follows:

$$\epsilon = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \phi_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \phi_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

The multiplication table of S_3 appears in Fig. 12-4.

MAP(A), PERM(A), and AUT(A)

Let A be a nonempty set. The collection $\mathrm{MAP}(A)$ of all functions (mappings) $f: A \to A$ is a semigroup under composition of functions; it is not a group since some functions may have no inverses. However, the subsemigroup $\mathrm{PERM}(A)$ of all one-to-one correspondences of A with itself (called *permutations* of A) is a group under composition of functions.

Furthermore, suppose A contains some type of geometric or algebraic structure; for example, A may be the set of vertices of a graph, or A may be an ordered set or a semigroup. Then the set $\mathrm{AUT}(A)$ of all isomorphisms of A with itself (called *automorphisms* of A) is also a group under compositions of functions.

12.5 SUBGROUPS, NORMAL SUBGROUPS, AND HOMOMORPHISMS

Let H be a subset of a group G. Then H is called a *subgroup* of G if H itself is a group under the operation of G. Simple criteria to determine subgroups follow.

Proposition 12.5: A subset H of a group G is a subgroup of G if:
(i) the identity element $e \in H$;
(ii) H is closed under the operation of G, i.e. if $a, b \in H$, then $ab \in H$; and
(iii) H is closed under inverses, that is, if $a \in H$, then $a^{-1} \in H$.

Every group G has the subgroups $\{e\}$ and G itself. Any other subgroup of G is called a *nontrivial subgroup*.

Cosets

If H is a subgroup of G and $a \in G$, then the set

$$Ha = \{ha : h \in H\}$$

is called a *right coset* of H. (Analogously, aH is called a *left coset* of H.) We have the following important results (proved in Problems 12.17 and 12.19).

Theorem 12.6: Let H be a subgroup of a group G. Then the right cosets Ha form a partition of G.

Theorem 12.7 (Lagrange): Let H be a subgroup of a finite group G. Then the order of H divides the order of G.

One can actually show that the number of right cosets of H in G, called the *index of H in G,* is equal to the number of left cosets of H in G; and both numbers are equal to $|G|$ divided by $|H|$.

Normal Subgroups

The following definition applies.

Definition: A subgroup H of G is a *normal* subgroup if $a^{-1}Ha \subseteq H$ for every $a \in G$. Equivalently, H is normal if $aH = Ha$ for every $a \in G$, i.e., if the right and left cosets coincide.

Note that every subgroup of an abelian group is normal.

The importance of normal subgroups comes from the following result (proved in Problem 12.24).

Theorem 12.8: Let H be a normal subgroup of a group G. Then the cosets of H form a group under coset multiplication

$$(aH)(bH) = abH$$

This group is called the *quotient group* and is denoted by G/H.

Suppose the operation in G is addition or, in other words, G is written additively. Then the cosets of a subgroup H of G are of the form $a + H$. Moreover, if H is a normal subgroup of G, then the cosets form a group under coset addition, that is,

$$(a + H) + (b + H) = (a + b) + H$$

EXAMPLE 12.12

(*a*) Consider the permutation group S_3 of degree 3 which is investigated above. The set $H = \{\epsilon, \sigma_1\}$ is a subgroup of S_3. Its right and left cosets follow:

Right Cosets	Left Cosets
$H = \{\epsilon, \sigma_1\}$	$H = \{\epsilon, \sigma_1\}$
$H\phi_1 = \{\phi_1, \sigma_2\}$	$\phi_1 H = \{\phi_1, \sigma_3\}$
$H\phi_2 = \{\phi_2, \sigma_3\}$	$\phi_2 H = \{\phi_2, \sigma_2\}$

Observe that the right cosets and the left cosets are distinct; hence H is not a normal subgroup of S_3.

(*b*) Consider the group G of 2×2 matrices with rational entries and nonzero determinant. [See Example 12.11(*c*).] Let H be the subset of G consisting of matrices whose upper-right entry is zero; i.e., matrices of the form

$$\begin{pmatrix} a & 0 \\ c & d \end{pmatrix}$$

Then H is a subgroup of G since H is closed under multiplication and inverses and $I \in H$. However, H is not a normal subgroup since, for example,

$$\begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix}^{-1} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix} = \begin{pmatrix} -1 & -4 \\ 1 & 3 \end{pmatrix}$$

does not belong to H.

On the other hand, let K be the subset of G consisting of matrices with determinant 1. One can show that K is also a subgroup of G. Moreover, for any matrix X in G and any matrix A in K, we have

$$\det(X^{-1}AX) = 1$$

Hence $X^{-1}AX$ belongs to K, so K is a normal subgroup of G.

Integers Modulo *m*

Consider the group $\mathbf{Z}$ of integers under addition. Let H denote the multiples of 5, that is,

$$H = \{\ldots, -10, -5, 0, 5, 10, \ldots\}$$

Then H is a subgroup (necessarily normal) of $\mathbf{Z}$. The cosets of H in $\mathbf{Z}$ follow:

$$\bar{0} = 0 + H = H = \{\ldots, -10, -5, 0, 5, 10, \ldots\}$$
$$\bar{0} = 1 + H = \{\ldots, -9, -4, 1, 6, 11, \ldots\}$$
$$\bar{2} = 2 + H = \{\ldots, -8, -3, 2, 7, 12, \ldots\}$$
$$\bar{3} = 3 + H = \{\ldots, -7, -2, 3, 8, 13, \ldots\}$$
$$\bar{4} = 4 + H = \{\ldots, -6, -1, 4, 9, 14, \ldots\}$$

By the above Theorem 12.8, $\mathbf{Z}/H = \{0, 1, 2, 3, 4\}$ is a group under coset addition; its addition table appears in Fig. 12-5.

This quotient group $\mathbf{Z}/H$ is referred to as the integers modulo 5 and is frequently denoted by $\mathbf{Z}_5$. Analogously, for any positive integer n, there exists the quotient group $\mathbf{Z}_n$ called the integers modulo n.

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

Fig. 12-5

Cyclic Subgroups

Let G be any group and let a be any element of G. As usual, we define $a^0 = e$ and $a^{n+1} = a^n \cdot a$. Clearly, $a^m \cdot a^n = a^{m+n}$ and $(a^m)^n = a^{mn}$, for any integers m and n. All the powers of a,

$$\ldots, a^{-3}, a^{-2}, a^{-1}, e, a, a^2, a^3, \ldots$$

form a subgroup of G called the *cyclic group* generated by a, and will be denoted by $gp(a)$. Suppose that the powers of a are not distinct, say $a^r = a^s$ with, say, $r > s$. Then $a^{r-s} = e$ where $r - s > 0$. The smallest positive integer m such that $a^m = e$ is called the *order* of a and will be denoted by $|a|$. If $|a| = m$, then its cyclic subgroup $gp(a)$ has m elements given by

$$gp(a) = \{e, a, a^2, a^3, \ldots, a^{m-1}\}$$

For example, consider the element ϕ_1 in the symmetric group S_3 discussed above. We have

$$\phi_1^1 = \phi_1, \qquad \phi_1^2 = \phi_2, \qquad \phi_1^3 = \phi_2 \cdot \phi_1 = \epsilon$$

Hence $|\phi_1| = 3$ and $gp(\phi_1) = \{e, \phi_1, \phi_2, \}$. Observe that $|\phi_1|$ divides the order of S_3. This is true in general; that is, for any element a in a group G we have that $|a|$ equals the order of $gp(a)$ which divides $|G|$ by Lagrange's Theorem 12.7. We also remark that a group G is said to be *cyclic* if it has an element a such that $G = gp(a)$.

Generating Sets, Generators

Consider any subset A of a group G. Let $gp(A)$ denote the set of all elements x in G such that x is equal to a product of elements where each element comes from the set $A \cup A^{-1}$ (where A^{-1} denotes the set of inverses of elements of A). That is,

$$gp(A) = \{x \in G: x = b_1 b_2 \cdots b_m \text{ where each } b_i \in A \cup A^{-1}\}$$

Then $gp(A)$ is a subgroup of G with *generating set* A. In particular, A is said to *generate* the group G if

$G = gp(A)$, that is, if every g in G is a product of elements from $A \cup A^{-1}$. We say A is a *minimal set of generators* of G if A generates G and if no set with fewer elements than A generates G. For example, the permutations $a = \sigma_1$ and $b = \phi_1$ form a minimal set of generators of the symmetric group S_3 (Fig. 12-4) since:

$$\epsilon = a^2, \qquad \sigma_1 = a, \qquad \sigma_2 = ab, \qquad \sigma_3 = ab^2, \qquad \phi_1 = b, \qquad \phi_2 = b^2$$

and moreover, S_3 is not cyclic and so it cannot be generated by one element.

Homomorphisms

A mapping f from a group G into a group G' is called a *homomorphism* if

$$f(ab) = f(a)f(b)$$

for every $a, b \in G$. In addition, if f is one-to-one and onto, then f is called an *isomorphism* and G and G' are said to be *isomorphic*, written $G \simeq G'$.

If $f: G \to G'$ is a homomorphism, then the kernel of f, written $\mathrm{Ker} f$, is the set of elements whose image is the identity element e' of G'; that is,

$$\mathrm{Ker} f = \{a \in G : f(a) = e'\}$$

Recall that the image of f, written $f(G)$ or $\mathrm{Im} f$, consists of the images of the elements under f; that is,

$$\mathrm{Im} f = \{b \in G' : \text{there exists } a \in G \text{ for which } f(a) = b\}.$$

The following theorem (proved in Problem 12.21) is fundamental to group theory.

Theorem 12.9: Let $f: G \to G'$ be a homomorphism with kernel K. Then K is a normal subgroup of G, and the quotient group G/K is isomorphic to $f(G)$.

EXAMPLE 12.13

(*a*) Let G be the group of real numbers under addition, and let G' be the group of positive real numbers under multiplication. The mapping $f: G \to G'$ defined by $f(a) = 2^a$ is a homomorphism because

$$f(a + b) = 2^{a+b} = 2^a 2^b = f(a)f(b)$$

In fact, f is also one-to-one and onto; hence G and G' are isomorphic.

(*b*) Let G be the group of nonzero complex numbers under multiplication, and let G' be the group of nonzero real numbers under multiplication. The mapping $f: G \to G'$ defined by $f(z) = |z|$ is a homomorphism because

$$f(z_1 z_2) = |z_1 z_2| = |z_1|\,|z_2| = f(z_1)f(z_2)$$

The kernel K of f consists of those complex numbers z on the unit circle, i.e., for which $|z| = 1$. Thus G/K is isomorphic to the image of f, i.e., to the group of positive real numbers under multiplication.

(*c*) Let a be any element in a group G. The function $f: \mathbf{Z} \to G$ defined by $f(n) = a^n$ is a homomorphism since

$$f(m + n) = a^{m+n} = a^m \cdot a^n = f(m) \cdot f(n)$$

The image of f is $gp(a)$, the cyclic subgroup generated by a. By Theorem 12.9.

$$gp(a) \simeq \mathbf{Z}/K$$

where K is the kernel of F. If $K = \{0\}$, then $gp(a) \simeq \mathbf{Z}$. On the other hand, if m is the order of a, then $K = \{\text{multiples of } m\}$, and so $gp(a) \simeq \mathbf{Z}_m$. In other words, any cyclic group is isomorphic to either the integers $\mathbf{Z}$ under addition, or to $\mathbf{Z}_m$, the integers under addition modulo m.

12.6 RINGS, INTEGRAL DOMAINS, AND FIELDS

Let R be a nonempty set with two binary operations, an operation of addition (denoted by $+$) and an operation of multiplication (denoted by juxtaposition). Then R is called a *ring* if the following axioms are satisfied:

$[\mathbf{R}_1]$ For any $a, b, c \in R$, we have $(a + b) + c = a + (b + c)$.
$[\mathbf{R}_2]$ There exists an element $0 \in R$, called the *zero* element, such that $a + 0 = 0 + a = a$ for every $a \in R$.
$[\mathbf{R}_3]$ For each $a \in R$ there exists an element $-a \in R$, called the *negative* of a, such that $a + (-a) = (-a) + a = 0$.
$[\mathbf{R}_4]$ For any $a, b \in R$, we have $a + b = b + a$.
$[\mathbf{R}_5]$ For any $a, b, c \in R$, we have $(ab)c = a(bc)$.
$[\mathbf{R}_6]$ For any $a, b, c \in R$, we have (i) $a(b + c) = ab + ac$, and (ii) $(b + c)a = ba + ca$.

Observe that the axioms $[\mathbf{R}_1]$ through $[\mathbf{R}_4]$ may be summarized by saying that R is an abelian group under addition.

Subtraction is defined in R by $a - b \equiv a + (-b)$.

It can be shown (see Problem 12.29) that $a \cdot 0 = 0 \cdot a = 0$ for every $a \in R$.

A subset S of R is a *subring* of R if S itself is a ring under the operations in R. We note that S is a subring of R if (i) $0 \in S$, and (ii) for any $a, b \in S$, we have $a - b \in S$ and $ab \in S$.

Special Kinds of Rings: Integral Domains and Fields

This subsection defines a number of different kinds of rings, including integral domains and fields.

R is called a *commutative ring* if $ab = ba$ for every $a, b \in R$.

R is called a *ring with an identity element* 1 if the element 1 has the property that $a \cdot 1 = 1 \cdot a = a$ for every element $a \in R$. In such a case, an element $a \in R$ is called a *unit* if a has a *multiplicative inverse*, that is, an element a^{-1} in R such that $aa^{-1} = a^{-1}a = 1$.

R is called a *ring with zero divisors* if there exist nonzero elements $a, b \in R$ such that $ab = 0$. In such a case, a and b are called *zero divisors*.

Definition: A commutative ring R is an *integral domain* if R has no zero divisors, i.e., if $ab = 0$ implies $a = 0$ or $b = 0$.

Definition: A commutative ring R with an identity element 1 (not equal to 0) is a *field* if every nonzero $a \in R$ is a unit, i.e., has a multiplicative inverse.

A field is necessarily an integral domain; for if $ab = 0$ and $a \neq 0$, then

$$b = 1 \cdot b = a^{-1}ab = a^{-1} \cdot 0 = 0$$

We remark that a field may also be viewed as a commutative ring in which the nonzero elements form a group under multiplication.

EXAMPLE 12.14

(*a*) The set $\mathbf{Z}$ of integers with the usual operations of addition and multiplication is the classical example of an integral domain (with an identity element). The units in $\mathbf{Z}$ are only 1 and -1, that is, no other element in $\mathbf{Z}$ has a multiplicative inverse.

(*b*) The set $\mathbf{Z}_m = \{0, 1, 2, \ldots, m - 1\}$ under the operation of addition and multiplication modulo m is a ring; it is called the *ring of integers modulo m*. If m is a prime, then $\mathbf{Z}_m$ is a field. On the other hand, if m is not a prime then $\mathbf{Z}_m$ has zero divisors. For instance, in the ring $\mathbf{Z}_6$.

$$2 \cdot 3 = 0 \qquad \text{but} \qquad 2 \neq 0 \pmod 6 \qquad \text{and} \qquad 3 \neq 0 \pmod 6$$

(*c*) The rational numbers **Q** and the real numbers **R** each form a field with respect to the usual operations of addition and multiplication.

(*d*) Let M denote the set of 2×2 matrices with integer or real entries. Then M is a noncommutative ring with zero divisors under the operations of matrix addition and matrix multiplication. M does have an identity element, the identity matrix.

(*e*) Let R be any ring. Then the set $R[x]$ of all polynomials over R is a ring with respect to the usual operations of addition and multiplication of polynomials. Moreover, if R is an integral domain then $R[x]$ is also an integral domain.

Ideals

A subset J of a ring R is called an *ideal* in R if the following three properties hold:

(i) $0 \in J$.

(ii) For any $a, b \in J$, we have $a - b \in J$.

(iii) For any $r \in R$ and $a \in J$, we have $ra,\ ar \in J$.

Note first that J is a subring of R. Also, J is a subgroup (necessarily normal) of the additive group of R. Thus we can form the collection of cosets

$$\{a + J : a \in R\}$$

which forms a partition of R.

The importance of ideals comes from the following theorem which is analogous to Theorem 12.7 for normal subgroups.

Theorem 12.10: Let J be an ideal in a ring R. Then the cosets $\{a + J : a \in R\}$ form a ring under the coset operations

$$(a + J) + (b + J) = a + b + J \qquad \text{and} \qquad (a + J)(b + J) = ab + J$$

This ring is denoted by R/J and is called the *quotient ring*.

Now let R be a commutative ring with an identity element 1. For any $a \in R$, the set $(a) = \{ra : r \in R\} = aR$ is an ideal, it is called the *principal ideal* generated by a. If every ideal in R is a principal ideal, then R is called a *principal ideal ring*. In particular, if R is also an integral domain, then R is called a *principal ideal domain* (PID).

EXAMPLE 12.15

(*a*) Consider the ring **Z** of integers. Then every ideal J in **Z** is a principal ideal, that is, $J = (m) = m\mathbf{Z}$, for some integer m. Thus **Z** is a *principal ideal domain* (PID). The quotient ring $\mathbf{Z}_m = \mathbf{Z}/(m)$ is simply the ring of integers modulo m. Although, **Z** is an integral domain (no zero divisors), the quotient ring $\mathbf{Z}_m$ may have zero divisors, e.g., 2 and 3 are zero divisors in $\mathbf{Z}_6$.

(*b*) Let R be any ring. Then $\{0\}$ and R are ideals. In particular, if R is a field, then $\{0\}$ and R are the only ideals.

(*c*) Let K be a field. Then the ring $K[x]$ of polynomials over K is a PID (principal ideal domain). On the other hand, the ring $K[x, y]$ of polynomials in two variables is not a PID.

(*d*) Let M be the ring of 2×2 matrices with integer entries. Let J consists of all matrices of the form

$$\begin{bmatrix} 0 & a \\ 0 & b \end{bmatrix}$$

Note that: (i) $0 \in J$. (ii) For any $a, b \in J$, we have $a - b \in J$. (iii) For any $r \in M$ and $a \in J$, we have $ra \in J$; that is, $RJ \subseteq J$. However, $JR \not\subseteq J$. Thus J is not an ideal. (It is called a *left ideal*.)

Ring Homomorphisms

A mapping f from a ring R into a ring R' is called a *ring homomorphism* or, simply, *homomorphism* if

$$f(a+b) = f(a) + f(b), \qquad f(ab) = f(a)f(b)$$

for every $a, b \in R$. In addition, if f is one-to-one and onto, then f is called an *isomorphism* and R and R' are said to be *isomorphic*, written $R \simeq R'$.

If $f: R \to R'$ is a homomorphism, then the kernel of f, written $\mathrm{Ker} f$, is the set of elements whose image is the zero element 0 of R'; that is,

$$\mathrm{Ker} f = \{r \in R: f(r) = 0\}$$

The following theorem (analogous to Theorem 12.9 for groups) is fundamental to ring theory.

Theorem 12.11: Let $f: R \to R'$ be a ring homomorphism with kernel K. Then K is an ideal in R, and the quotient ring R/K is isomorphic to $f(R)$.

Divisibility in Integral Domains

Now let D be an integral domain. We say that b *divides* a in D if $a = bc$ for some $c \in D$. An element $u \in D$ is called a *unit* if u divides 1, i.e., if u has a multiplicative inverse. An element $b \in D$ is called an *associate* of $a \in D$ if $b = ua$ for some unit $u \in D$. A nonunit $p \in D$ is said to be *irreducible* if $p = ab$ implies a or b is a unit.

An integral domain D is called a *unique factorization domain* (UFD) if every nonunit $a \in D$ can be written uniquely (up to associates and order) as a product of irreducible elements.

EXAMPLE 12.16

(*a*) The ring $\mathbf{Z}$ of integers is the classical example of a unique factorization domain. The units of $\mathbf{Z}$ are 1 and -1. The only associates of $n \in \mathbf{Z}$ are n and $-n$. The irreducible elements of $\mathbf{Z}$ are the prime numbers.

(*b*) The set $D = \{a + b\sqrt{13} : a, b \text{ integers}\}$ is an integral domain. The units of D are ± 1, $18 \pm 5\sqrt{13}$ and $-18 \pm 5\sqrt{13}$. The elements 2, $3 - \sqrt{13}$ and $-3 - \sqrt{13}$ are irreducible in D. Observe that

$$4 = 2 \cdot 2 = (3 - \sqrt{13})(-3 - \sqrt{13})$$

Thus D is not a unique factorization domain. (See Problem 12.99.)

12.7 POLYNOMIALS OVER A FIELD

This section investigates polynomials whose coefficients come from some integral domain or field K. In particular, we show that polynomials over a field K have many of the same properties as the integers.

Basic Definitions

Let K be an integral domain or a field. Formally, a *polynomial f over K* is an infinite sequence of elements from K in which all except a finite number of them are 0; that is,

$$f = (\ldots, 0, a_n, \ldots, a_1, a_0) \qquad \text{or, equivalently,} \qquad f(t) = a_n t^n + \cdots + a_0$$

where the symbol t is used as an indeterminate. The entry a_k is called the *kth coefficient* of f. If n is the largest integer for which $a_n \neq 0$, then we say that the *degree* of f is n, written $\deg(f) = n$. We also call a_n the *leading coefficient* of f, and, if $a_n = 1$, we call f a *monic* polynomial. On the other hand, if every coefficient of f is 0 then f is called the *zero polynomial*, written $f \equiv 0$. The degree of the zero polynomial is not defined.

Let $K[t]$ be the collection of all polynomials $f(t)$ over K. Addition and multiplication are defined in $K[t]$ as follows. Suppose

$$f(t) = a_n t^n + \cdots + a_0 \qquad \text{and} \qquad g(t) = b_m t^m + \cdots + b_0$$

Then the *sum* $f + g$ is the polynomial obtained by adding corresponding coefficients; that is, if $m \leq n$, then

$$f(t) + g(t) = a_n t^n + \cdots + (a_m + b_m)t^m + \cdots + (a_1 + b_1)t + (a_0 + b_0)$$

Furthermore, the product of f and g is the polynomial

$$f(t)g(t) = (a_n b_m)t^{n+m} + \cdots + (a_1 b_0 + a_0 b_1)t + (a_0 b_0)$$

That is,

$$f(t)g(t) = c_{n+m}t^{n+m} + \cdots + c_1 t + c_0 \qquad \text{where} \qquad c_k = \sum_{i=0}^{k} a_i b_{k-1} = a_0 b_k + a_1 b_{k-1} + \cdots + a_k b_0$$

The set K of *scalars* is viewed as a subset of $K[t]$. Specifically, we identify the scalar $a_0 \in K$ with the polynomial

$$f(t) = a_0 \qquad \text{or} \qquad a_0 = (\ldots, 0, 0, a_0)$$

Then the operators of addition and scalar multiplication are preserved by this identification; that is,

$$(\ldots, 0, a_0) + (\ldots, 0, b_0) = (\ldots, 0, a_0 + b_0) \qquad \text{and} \qquad (\ldots, 0, a_0) \cdot (\ldots, 0, a_0 b_0) = (\ldots, 0, a_0 b_0)$$

Thus, the mapping $\Psi\colon K \to K[t]$ defined by $\Psi(a_0) = a_0$ is an isomorphism which embeds K into $K[t]$.

Theorem 12.12: Let K be an integral domain. The $K[t]$ under the operations of addition and multiplication of polynomials is a commutative ring with an identity element 1.

The following simple result has important consequences.

Lemma 12.13: Suppose f and g are polynomials over an integral domain K. Then

$$\deg(fg) = \deg(f) + \deg(g)$$

The proof follows directly from the definition of the product of polynomials. That is, suppose $f(t) = a_n t^n + \cdots + a_0$ and $g(t) = b_m t^m + \cdots + b_0$, where $a_n \neq 0$ and $b_m \neq 0$. Then

$$f(t)g(t) = a_n b_m t^{m+n} + \text{ terms of lower degree}$$

Also, since K is an integral domain with no zero divisors, $a_n b_m \neq 0$. Thus

$$\deg(fg) = m + n = \deg(f) + \deg(g)$$

and the lemma is proved.

The following proposition lists many properties of our polynomials. [Recall that a polynomial g is said to *divide* a polynomial f if there exists a polynomial h such that $f(t) = g(t)h(t)$.]

Proposition 12.14: Let K be an integral domain and let f and g be polynomials over K.

(i) $K[t]$ is an integral domain.

(ii) The units of $K[t]$ are the units in K.

(iii) If g divides f, then $\deg(g) \leq \deg(f)$ or $f \equiv 0$.

(iv) If g divides f and f divides g, then $f(t) = kg(t)$ where k is a unit in K.

(v) If d and d' are monic polynomials such that d divides d' and d' divides d, then $d = d'$.

Euclidean Algorithm, Roots of Polynomials

This subsection discusses the roots of a polynomial $f(t)$, where we now assume the coefficients of $f(t)$ come from a field K. Recall that a scalar $a \in K$ is a *root* of a polynomial $f(t)$ if $f(a) = 0$. First we begin with an important theorem which is very similar to a corresponding theorem for the integers **Z**.

Theorem 12.15 (Euclidean Division Algorithm): Let $f(t)$ and $g(t)$ be polynomials over a field K with $g(t) \neq 0$. Then there exist polynomials $q(t)$ and $r(t)$ such that

$$f(t) = q(t)g(t) + r(t)$$

where either $r(t) \equiv 0$ or $\deg(r) < \deg(g)$.

The above theorem (Proved in Problem 12.39) formalizes the process known as "long division". The polynomial $q(t)$ is called the *quotient* and the polynomial $r(t)$ is called the *remainder* when $f(t)$ is divided by $g(t)$.

Corollary 12.16 (Remainder Theorem): Suppose $f(t)$ is divided by $g(t) = t - a$. Then $f(a)$ is the remainder.

The proof follows from the Euclidean Algorithm. That is, dividing $f(t)$ by $t - a$ we get

$$f(t) = q(t)(t - a) + r(t)$$

where $\deg(r) < \deg(t - a) = 1$. Hence $r(t) = r$ is a scalar. Substituting $t = a$ in the equation for $f(t)$ yields

$$f(a) = q(a)(a - a) + r = q(t) \cdot 0 + r = r$$

Thus $f(a)$ is the remainder, as claimed.

Corollary 12.16 also tells us that $f(a) = 0$ if and only if the remainder $r = r(t) \equiv 0$. Accordingly:

Corollary 12.17 (Factor Theorem): The scalar $a \in K$ is a root of $f(t)$ if and only if $t - a$ is a factor of $f(t)$.

The next theorem tells us the number of possible roots of a polynomial.

Theorem 12.18: Suppose $f(t)$ is a polynomial over a field K, and $\deg(f) = n$. Then $f(t)$ has at most n roots.

The following theorem is the main tool for finding rational roots of a polynomial with integer coefficients.

Theorem 12.19: Suppose a rational number p/q (reduced to lowest terms) is a root of the polynomial

$$f(t) = a_n t^n + \cdots + a_1 t + a_0$$

where all the coefficients $a_n, \ldots, a_1, a_0$ are integers. Then p divides the constant term a_0 and q divides the leading coefficient a_n. In particular, if $c = p/q$ is an integer, then c divides the constant term a_0.

EXAMPLE 12.17

(*a*) Suppose $f(t) = t^3 + t^2 - 8t + 4$. Assuming $f(t)$ has a rational root, find all the roots of $f(t)$.

Since the leading coefficient is 1, the rational roots of $f(t)$ must be integers from among ± 1, ± 2, ± 4. Note $f(1) \neq 0$ and $f(-1) \neq 0$. By synthetic division, or dividing by $t - 2$, we get

$$\begin{array}{r|rrrrrr} 2 & 1 & + & 1 & - & 8 & + & 4 \\ & & & 2 & + & 6 & - & 4 \\ \hline & 1 & + & 3 & - & 2 & + & 0 \end{array}$$

Therefore $t = 2$ is a root and $f(t) = (t-2)(t^2 + 3t - 2)$. Using the quadratic formula for $t^2 + 3t - 2 = 0$, we obtain the following roots of $f(t)$:

$$t = 2, \qquad t = (-3 + \sqrt{17})/2, \qquad t = (-3 - \sqrt{17})/2$$

(*b*) Suppose $h(t) = t^4 - 2t^3 + 11t - 10$. Find all the real roots of $h(t)$ assuming there are two integer roots.

The integer roots must be among ± 1, ± 2, ± 5, ± 10. By synthetic division (or dividing by $t - 1$ and then $t + 2$) we get

$$\begin{array}{r|rrrrrrrr} 1 & 1 & - & 2 & + & 0 & + & 11 & - & 10 \\ & & & 1 & - & 1 & - & 1 & + & 10 \\ \hline -2 & 1 & - & 1 & - & 1 & + & 10 & + & 0 \\ & & - & 2 & + & 6 & - & 10 & & \\ \hline & 1 & - & 3 & + & 5 & + & 0 & & \end{array}$$

Thus $t = 1$ and $t = -2$ are roots and $h(t) = (t-1)(t+2)(t^2 - 3t + 5)$. The quadratic formula with $t^2 - 3t + 5$ tells us that there are no other real roots. That is, $t = 1$ and $t = -2$ are the only real roots of $h(t)$.

K[*t*] as a PID and UFD

The following theorems apply.

Theorem 12.20: The ring $K[t]$ of polynomials over a field K is a principal ideal domain (PID). If J is an ideal in $K[t]$, then there exists a unique monic polynomial d which generates J, that is, every polynomial f in J is a multiple of d.

Theorem 12.21: Let f and g be polynomials in $K[t]$, not both zero. Then there exists a unique monic polynomial d such that:
(i) d divides both f and g.
(ii) If d' divides f and g, then d' divides d.

The polynomial d in the above theorem is called the *greatest common divisor* of f and g, written $d = \gcd(f, g)$. If $d = 1$, then f and g are said to be *relatively prime*.

Corollary 12.22: Let d be the greatest common divisor of f and g. Then there exist polynomials m and n such that $d = mf + ng$. In particular, if f and g are relatively prime, then there exist polynomials m and n such that $mf + ng = 1$.

A polynomial $p \in K[t]$ is said to be *irreducible* if p is not a scalar and if $p = fg$ implies f or g is a scalar. In other words, p is irreducible if its only divisors are its associates (scalar multiples).

Lemma 12.23: Suppose $p \in K[t]$ is irreducible. If p divides the product fg of polynomials f and g in $K[t]$, then p divides f or p divides g. More generally, if p divides the product $f_1 f_2 \cdots f_n$ of n polynomials, then p divides one of them.

The next theorem states that the polynomials over a field form a unique factorization domain (UFD).

Theorem 12.24 (Unique Factorization Theorem): Let f be a nonzero polynomial in $K[t]$. Then f can be written uniquely (except for order) as a product

$$f = kp_1 p_2 \cdots p_n$$

where $k \in K$ and the p's are monic irreducible polynomials in $K[t]$.

Fundamental Theorem of Algebra

The proof of the following theorem lies beyond the scope of this text.

Fundamental Theorem of Algebra: Any nonzero polynomial $f(t)$ over the complex field **C** has a root in **C**. Thus $f(t)$ can be written uniquely (except for order) as a product

$$f(t) = k(t - r_1)(t - r_2) \cdots (t - r_n)$$

where k and the r_i are complex numbers and $\deg(f) = n$.

The above theorem is certainly not true for the real field **R**. For example, $f(t) = t^2 + 1$ is a polynomial over **R**, but $f(t)$ has no real root.

The following theorems apply.

Theorem 12.25: Suppose $f(t)$ is a polynomial over the real field **R**, and suppose the complex number $z = a + bi$, $b \neq 0$, is a root of $f(t)$. Then the complex conjugate $\bar{z} = a - bi$ is also a root of $f(t)$. Hence

$$c(t) = (t - z)(t - \bar{z}) = t^2 - 2at + a^2 + b^2$$

is a factor of $f(t)$.

Theorem 12.26: Let $f(t)$ be a nonzero polynomial over the real field **R**. Then $f(t)$ can be written uniquely (except for order) as a product

$$f(t) = kp_1(t)p_2(t) \cdots p_m(t)$$

where $k \in \mathbf{R}$ and the $p_i(t)$ are real monic polynomials of degree 1 or 2.

EXAMPLE 12.18 Let $f(t) = t^4 - 3t^3 + 6t^2 + 25t - 39$. Find all the roots of $f(t)$ given that $t = 2 + 3i$ is a root.

Since $2 + 3i$ is a root, then $2 - 3i$ is a root and $c(t) = t^2 - 4t + 13$ is a factor of $f(t)$. Dividing $f(t)$ by $c(t)$ we get

$$f(t) = (t^2 - 4t + 13)(t^2 + t - 3)$$

The quadratic formula with $t^2 + t - 3$ gives us the other roots of $f(t)$. That is, the four roots of $f(t)$ are as follows:

$$t = 2 + 3i, \qquad t = 2 - 3i, \qquad t = (-1 + \sqrt{13})/2, \qquad t = (-1 - \sqrt{13})/2$$

Solved Problems

OPERATIONS AND SEMIGROUPS

12.1. Consider the set **N** of positive integers, and let $*$ denote the operation of least common multiple (lcm) on **N**.

(*a*) Find $4 * 6$, $3 * 5$, $9 * 18$, and $1 * 6$.

(*b*) Is $(\mathbf{N}, *)$ a semigroup? Is it commutative?

(*c*) Find the identity element of $*$.

(*d*) Which elements in **N**, if any, have inverses and what are they?

(*a*) Since $x * y$ means the least common multiple of x and y, we have:

$$4 * 6 = 12, \qquad 3 * 5 = 15, \qquad 9 * 18 = 18, \qquad 1 * 6 = 6$$

(*b*) One proves in number theory that $(a * b) * c = a * (b * c)$, i.e., that the operation of lcm is associative, and that $a * b = b * a$, i.e., that the operation of lcm is commutative. Hence $(\mathbf{N}, *)$ is a commutative semigroup.

(*c*) The integer 1 is the identity element since $\text{lcm}\,(1, a) = a$ for any positive integer a, i.e., $1 * a = a * 1 = a$ for any $a \in \mathbf{N}$.

(*d*) Since $\text{lcm}(a, b) = 1$ if and only if $a = 1$ and $b = 1$, the only number which has an inverse is 1 and it is its own inverse.

12.2. Consider the set $\mathbf{Q}$ of rational numbers, and let $*$ be the operation on $\mathbf{Q}$ defined by

$$a * b = a + b - ab$$

(*a*) Find $3 * 4,\ 2 * (-5)$ and $7 * \frac{1}{2}$.

(*b*) Is $(\mathbf{Q}, *)$ a semigroup? Is it commutative?

(*c*) Find the identity element for $*$.

(*d*) Do any of the elements in $\mathbf{Q}$ have an inverse? What is it?

(*a*) $3 * 4 = 3 + 4 - 3 \cdot (4) = 3 + 4 - 12 = -5.$
$2 * (-5) = 2 + (-5) - 2 \cdot (-5) = 2 - 5 + 10 = 7.$
$7 * \frac{1}{2} = 7 + \frac{1}{2} - 7(\frac{1}{2}) = 4.$

(*b*) We have:

$$\begin{aligned}(a * b) * c &= (a + b - ab) * c \\ &= (a + b - ab) + c - (a + b - ab)c \\ &= a + b - ab + c - ac - bc + abc \\ &= a + b + c - ab - ac - bc + abc\end{aligned}$$

$$\begin{aligned}a * (b * c) &= a * (b + c - bc) \\ &= a + (b + c - bc) - a(b + c - bc) \\ &= a + b + c - bc - ab - ac + abc\end{aligned}$$

Hence $*$ is associative and $(\mathbf{Q}, *)$ is a semigroup. Also,

$$a * b = a + b - ab = b + a - ba = b * a$$

Hence $(\mathbf{Q}, *)$ is a commutative semigroup.

(*c*) An element e is an identity element if $a * e = a$ for every $a \in \mathbf{Q}$. Compute as follows:

$$a * e = a, \qquad a + e - ae = a, \qquad e - ea = 0, \qquad e(1 - a) = 0, \qquad e = 0$$

Accordingly, 0 is the identity element.

(*d*) In order for e to have an inverse x, we must have $a * x = 0$ since 0 is the identity element by Part (*e*). Compute as follows:

$$a * x = 0, \qquad a + x - ax = 0, \qquad a = ax - x, \qquad a = x(a - 1), \qquad x = a/(a - 1)$$

Thus if $a \neq 1$, then a has an inverse and it is $a/(a - 1)$.

12.3. Let S be a semigroup with identity e, and let b and b' be inverses of a. Show that $b = b'$, that is, that inverses are unique if they exist.

We have:

$$b * (a * b') = b * e = b \qquad \text{and} \qquad (b * a) * b' = e * b' = b'$$

Since S is associative, $(b * a) * b' = b * (a * b')$; hence $b = b'$.

12.4. State whether or not each of the following six subsets of the positive integers $\mathbf{N}$ is closed under the operation of multiplication:

(*a*) $A = \{0, 1\}$.
(*b*) $B = \{1, 2\}$.
(*c*) $C = \{x: x \text{ is prime}\}$.
(*d*) $D = \{2, 4, 6, \ldots\} = \{x: x \text{ is even}\}$.
(*e*) $E = \{1, 3, 5, \ldots\} = \{x: x \text{ is odd}\}$.
(*f*) $F = \{2, 4, 8, \ldots\} = x: x = 2^n, n \in \mathbf{N}\}$.

Which of the six sets, if any, are closed under the operation of addition?

(*a*) We have:

$$0 \cdot 0 = 0, \qquad 0 \cdot 1 = 0, \qquad 1 \cdot 0 = 0, \qquad 1 \cdot 1 = 1$$

Hence A is closed under multiplication.

(*b*) Since $2 \cdot 2 = 4$, which does not belong to B, the set B is not closed under multiplication.

(*c*) Note that 2 and 3 are prime but $2 \cdot 3 = 6$ is not prime; hence C is not closed under multiplication.

(*d*) The product of even numbers is even; hence D is closed under multiplication.

(*e*) The product of odd numbers is odd; hence E is closed under multiplication.

(*f*) Since $2^r \cdot 2^s = 2^{r+s}$, F is closed under multiplication.

Since the sum of two even integers is even, the set D is closed under addition. However, each of the other sets is not closed under addition since, for example,

$$1 + 1 = 2 \notin A, \qquad 3 + 5 = 8 \notin C, \qquad 2 + 4 = 6 \notin F$$
$$1 + 2 = 3 \notin B, \qquad 1 + 3 = 4 \notin E$$

12.5. Let $S = \mathbf{N} \times \mathbf{N}$. Let $*$ be the operation on S defined by $(a, b) * (a', b') = (aa', bb')$.

(*a*) Show that $*$ is associative. (Hence S is a semigroup.)

(*b*) Define $f: (S, *) \to (\mathbf{Q}, \times)$ by $f(a, b) = a/b$. Show that f is a homomorphism.

(*c*) Find the congruence relation $\sim$ in S determined by the homomorphism f, i.e., $x \sim y$ if $f(x) = f(y)$. (See Theorem 12.4.)

(*d*) Describe $S/\sim$. Does $S/\sim$ have an identity element? Does it have inverses?

Suppose $x = (a, b), y = (c, d), z = (e, f)$.

(*a*) We have

$$(xy)z = (ac, bd) * (e, f) = [(ac)e, (bd)f]$$
$$x(yz) = (a, b) * (ce, df) = [a(ce), b(df)]$$

Since a, b, c, d, e, f, are positive integers, $(ac)e = a(ce)$ and $(bd)f = b(df)$

Thus $(xy)z = x(yz)$ and hence $*$ is associative. That is, $(S, *)$ is a semigroup.

(*b*) We have:

$$f(x * y) = f(ac, bd) = (ac)/(bd) = (a/b)(c/d) = f(x)f(y)$$

Thus f is a homomorphism.

(*c*) Suppose $f(x) = f(y)$. Then

$$\frac{a}{b} = \frac{c}{d} \text{ and hence } ad = bc.$$

Thus f determines the congruence relation $\sim$ on S defined by $(a, b) \sim (c, d)$ if $ad = bc$.

(*d*) The image of f is $\mathbf{Q}^+$, the set of positive rational numbers. By Theorem 12.3, $S/\sim$ is isomorphic to $\mathbf{Q}^+$. Thus $S/\sim$ does have an identity element, and every element has an inverse.

12.6. Let $S = \mathbf{N} \times \mathbf{N}$. Let $*$ be the operation on S defined by

$$(a, b) * (a', b') = (a + a', b + b')$$

(*a*) Show that $*$ is associative. (Hence S is a semigroup.)

(*b*) Define $f: (S, *) \to (\mathbf{Z}, +)$ by $f(\text{a,b}) = a - b$. Show that f is a homomorphism.

(*c*) Find the congruence relation $\sim$ in S determined by the homomorphism f, i.e., $x \sim y$ if $f(x) = f(y)$. (See Theorem 12.4.)

(*d*) Describe $S/\sim$. Does $S/\sim$ have an identity element? Inverses?

Suppose $x = (a, b)$, $y = (c, d)$, $z = (e, f)$.

(*a*) We have

$$(xy)z = (a + c, b + d) * (e, f) = [(a + c) + e, (b + d) + f]$$
$$x(yz) = (a, b) * (c + e, d + f) = [a + (c + e), b + (d + f)]$$

Since a, b, c, d, e, f are positive integers,

$$(a + c) + e = a + (c + e) \qquad \text{and} \qquad (b + d) + f = b + (d + f)$$

Thus $(xy)z = x(yz)$ and hence $*$ is associative. That is, $(S, *)$ is a semigroup.

(*b*) We have:

$$f(x * y) = f(a + c, b + d) = (a + c) - (b + d) = (a - b) + (c - d) = f(x)f(y)$$

Thus f is a homomorphism.

(*c*) Suppose $f(x) = f(y)$. Then $a - b = c - d$ and hence $a + d = b + d$. Thus f determines the congruence relation $\sim$ on S defined by

$$(a, b) \sim (c, d) \text{ if } a + d = b + c$$

(*d*) The image of f is all of $\mathbf{Z}$ since every integer is the difference of two positive integers. Therefore, by Theorem 12.3, $S/\sim$ is isomorphic to $\mathbf{Z}$. Thus $S/\sim$ does have an identity element, and every element has an (additive) inverse.

12.7. Prove Theorem 12.1: Suppose $*$ is an associative operation on a set S. Then any product $a_1 * a_2 * \cdots * a_n$ requires no parenthesis, that is, all possible products are equal.

The proof is by induction on n. Since n is associative, the theorem holds for $n = 1, 2$, and 3. Suppose $n \geq 4$. We use the notation:

$$(a_1 a_2, \cdots a_n) = (\cdots((a_1 a_2)a_3)\cdots)a_n \qquad \text{and} \qquad [a_1 a_2 \cdots a_n] = \text{any product}$$

We show $[a_1 a_2 \cdots a_n] = (a_1 a_2 \cdots a_n)$ and so all such products will be equal. Since $[a_1 a_2 \cdots a_n]$ denotes some product, there exists an $r < n$ such that $[a_1 a_2 \cdots a_n] = [a_1 a_2 \cdots a_r][a_{r+1} \cdots a_n]$. Therefore, by induction,

$$\begin{aligned}[a_1 a_2 \cdots a_n] &= [a_1 a_2 \cdots a_r][a_{r+1} \cdots a_n] = [a_1 a_2 \cdots a_r](a_{r+1} \cdots a_n) \\ &= [a_1 \cdots a_r]((a_{r+1} \cdots a_{n-1})a_n) = ([a_1 \cdots a_r](a_{r-1} \cdots a_{n-1}))a_n \\ &= [a_1 \cdots a_{n-1}]a_n = (a_1 \cdots a_{n-1})a_n = (a_1 a_2 \cdots a_n)\end{aligned}$$

Thus the theorem is proved.

12.8. Prove Theorem 12.4: Let $f: S \to S'$ be a semigroup homomorphism. Let $a \sim b$ if $f(a) = f(b)$. Then: (i) $\sim$ is a congruence relation, (ii) $S/\sim$ is isomorphic to $f(S)$.

(i) First we show that $\sim$ is an equivalence relation. Since $f(a) = f(a)$, we have $a \sim a$. If $a \sim b$, then $f(a) = f(b)$ or $f(b) = f(a)$ and hence $b \sim a$. Lastly, if $a \sim b$ and $b \sim c$, then $f(a) = f(b)$ and $f(b) = f(c)$, and hence $f(a) = f(c)$. Thus $a \sim c$. That is, $\sim$ is an equivalence relation. Suppose now $a \sim a'$ and $b \sim b'$. Then $f(a) = f(a')$ and $f(b) = f(b')$. Since f is a homomorphism,

$$f(ab) = f(a)f(b) = f(a')f(b') = f(a'b')$$

Therefore $ab \sim a'b'$. That is, $\sim$ is a congruence relation.

(ii) Define $\Psi: S/\sim \to f(S)$ by $\Psi([a]) = f(a)$. We need to prove: (1) Ψ is well-defined, that is, $\Psi([a]) \in f(S)$, and if $[a] = [b]$ then $f([a]) = f([b])$. (2) Ψ is an isomorphism, that is, Ψ is a homomorphism, one-to-one and onto.

(1) *Proof that Ψ is well-defined*: We have $\Psi([a]) = f(a)$. Since $a \in S$, we have $f(a) \in f(S)$. Hence $\Psi([a]) \in f(S)$, as required. Now suppose $[a] = [b]$. Then $a \sim b$ and hence $f(a) = f(b)$. Thus

$$\Psi([a]) = f(a) = f(b) = \Psi([b])$$

That is, Ψ is well-defined.

(2) *Proof that Ψ is an isomorphism*: Since f is a homomorphism,

$$\Psi([a][b]) = \Psi[ab] = f(ab) = f(a)f(b) = \Psi([a])\Psi([b])$$

Hence Ψ is a homomorphism. Suppose $\Psi([a]) = \Psi([b])$. Then $f(a) = f(b)$, and so $a \sim b$. Thus $[a] = [b]$ and Ψ is one-to-one. Lastly, let $y \in f(S)$. Then, $f(a) = y$ for some $a \in S$. Hence $\Psi([a]) = f(a) = y$. Thus Ψ is onto $f(S)$. Accordingly, Ψ is an isomorphism.

GROUPS

12.9. Consider the symmetric group S_3 whose multiplication table is given in Fig. 12-4.

(*a*) Find the order and the group generated by each element of S_3.

(*b*) Find the number and all subgroups of S_3.

(*c*) Let $A = \{\sigma_1, \sigma_2\}$ and $B = \{\phi_1, \phi_2\}$. Find AB, $\sigma_3 A$, and $A\sigma_3$.

(*d*) Let $H = gp(\sigma_1)$ and $K = gp(\sigma_2)$. Show that HK is not a subgroup of S_3.

(*e*) Is S_3 cyclic?

(*a*) There are six elements: (1) ϵ, (2) σ_1, (3) σ_2, (4) σ_3, (5) ϕ_1, (6) ϕ_2. Find the powers of each element x until $x^n = \epsilon$. Then $|x| = n$, and $gp(x) = \{\epsilon, x, x^2, \ldots, x^{n-1}\}$. Note $x^1 = x$, so we need only begin with $n = 2$ when $x \neq \epsilon$.

(1) $\epsilon^1 = \epsilon$; so $|\epsilon| = 1$ and $g(\epsilon) = \{\epsilon\}$.

(2) $\sigma_1^2 = \epsilon$; hence $|\sigma_1| = 2$ and $gp(\sigma_1) = \{\epsilon, \sigma_1\}$

(3) $\sigma_2^2 = \epsilon$; hence $|\sigma_2| = 2$ and $gp(\sigma_2) = \{\epsilon, \sigma_2\}$.

(4) $\sigma_3^2 = \epsilon$; hence $|\sigma_3| = 2$ and $gp(\sigma_3) = \{\epsilon, \sigma_3\}$.

(5) $\phi_1^2 = \phi_2$, $\phi_1^3 = \phi_2\phi_1 = \epsilon$; hence $|\phi_1| = 3$ and $gp(\phi_1) = \{\epsilon, \phi_1, \phi_2\}$.

(6) $\phi_2^2 = \phi_1$, $\phi_2^3 = \phi_1\phi_2 = \epsilon$; hence $|\phi_2| = 3$ and $gp(\phi_1) = \{\epsilon, \phi_2, \phi_1\}$.

(*b*) First of all, $H_1 = \{e\}$ and $H_2 = S_3$ are subgroups of S_3. Any other subgroup of S_3 must have order 2 or 3 since its order must divide $S_3 = 6$. Since 2 and 3 are prime numbers, these subgroups must be cyclic (Problem 12.65) and hence must appear in part (*a*). Thus the other subgroups of S_3 are

$$H_3 = \{e, \sigma_1\}, \qquad H_4 = \{e, \sigma_2\}, \qquad H_5 = \{e, \sigma_3\}, \qquad H_6 = \{e, \phi_1, \phi_2\}$$

Accordingly, S_3 has six subgroups.

(*c*) Multiply each element of A by each element of B:

$$\sigma_1\phi_1 = \sigma_2, \qquad \sigma_1\phi_2 = \sigma_3, \qquad \sigma_3,\phi_1 = \sigma_3 \qquad \sigma_2\phi_2 = \sigma_1$$

Hence $AB = \{\sigma_1, \sigma_2, \sigma_3\}$.

Multiply σ_3 by each element of A:

$$\sigma_3\sigma_1 = \phi_1, \qquad \sigma_3\sigma_2 = \phi_2, \qquad \text{hence} \qquad \sigma_3 A = \{\phi_1, \phi_2\}$$

Multiply each element of A by σ_3:

$$\sigma_1\sigma_3 = \phi_2, \qquad \sigma_2\sigma_3 = \phi_1, \qquad \text{hence} \qquad A\sigma_3 = \{\phi_1, \phi_2\}$$

(*d*) $H = \{e, \sigma_1\}$, $K = \{e, \sigma_2\}$ and then $HK = \{e, \sigma_1, \sigma_2, \phi_1\}$, which is not a subgroup of S_3 since HK has four elements.

(*e*) S_3 is not cyclic since S_3 is not generated by any of its elements.

12.10. Consider the group $G = \{1, 2, 3, 4, 5, 6\}$ under multiplication modulo 7.

(*a*) Find the multiplication table of G.

(*b*) Find $2^{-1}, 3^{-1}, 6^{-1}$.

(*c*) Find the orders and subgroups generated by 2 and 3.

(*d*) Is G cyclic?

(*a*) To find $a * b$ in G, find the remainder when the product ab is divided by 7. For example, $5 \cdot 6 = 30$ which yields a remainder of 2 when divided by 7; hence $5 * 6 = 2$ in G. The multiplication table of G appears in Fig. 12-6.

(*b*) Note first that 1 is the identity element of G. Recall that a^{-1} is that element of G such that $aa^{-1} = 1$. Hence $2^{-1} = 4$, $3^{-1} = 5$ and $6^{-1} = 6$.

(*c*) We have $2^1 = 2$, $2^2 = 4$, but $2^3 = 1$. Hence $|2| = 3$ and $gp(2) = \{1, 2, 4\}$. We have $3^1 = 3$, $3^2 = 2$, $3^3 = 6$, $3^4 = 4$, $3^5 = 5$, $3^6 = 1$. Hence $|3| = 6$ and $gp(3) = G$.

(*d*) G is cyclic since $G = gp(3)$.

*	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

Fig. 12-6

12.11. Let G be a reduced residue system modulo 15, say,

$$G = \{1, 2, 4, 7, 8, 11, 13, 14\}$$

(the set of integers between 1 and 15 which are coprime to 15). Then G is a group under multiplication modulo 15.

(*a*) Find the multiplication table of G.

(*b*) Find 2^{-1}, 7^{-1}, 11^{-1}.

(*c*) Find the orders and subgroups generated by 2, 7, and 11.

(*d*) Is G cyclic?

(*a*) To find $a * b$ in G, find the remainder when the product ab is divided by 15. The multiplication table appears in Fig. 12-7.

(*b*) The integers r and s are inverses if $r * s = 1$. Hence $2^{-1} = 8$, $7^{-1} = 13$, $11^{-1} = 11$.

(*c*) We have $2^2 = 4$, $2^3 = 8$, $2^4 = 1$. Hence $|2| = 4$ and $gp(2) = \{1, 2, 4, 8\}$. Also, $7^2 = 4$, $7^3 = 4 * 7 = 13$, $7^4 = 13 * 7 = 1$. Hence $|7| = 4$ and $gp(7) = \{1, 4, 7, 13\}$. Lastly, $11^2 = 1$. Hence $|11| = 2$ and $gp(11) = \{1, 11\}$.

(*d*) No, since no element generates G.

*	1	2	4	7	8	11	13	14
1	1	2	4	7	8	11	13	14
2	2	4	8	14	1	7	11	13
4	4	8	1	13	2	14	7	11
7	7	14	13	4	11	2	1	8
8	8	1	2	11	4	13	14	7
11	11	7	14	2	13	1	8	4
13	13	11	7	1	14	8	4	2
14	14	13	11	8	7	4	2	1

Fig. 12-7

12.12. Let σ and τ be the following elements of the symmetric group S_6:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 5 & 4 & 6 & 2 \end{pmatrix} \quad \text{and} \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 1 & 6 & 2 & 4 \end{pmatrix}$$

Find: $\tau\sigma$, $\sigma\tau$, σ^2, and σ^{-1}. (Since τ and σ are functions, $\tau\sigma$ means apply σ and then τ.)

The effect of σ and then τ on $1, 2, \ldots, 6$ is pictured in Fig. 12-8(*a*); the effect of τ and then σ on $1, 2, \ldots, 6$ is pictured in Fig. 12-8(*b*); and the effect of σ and then σ again on $1, 2, \ldots, 6$ is pictured in Fig. 12-8(*c*). Thus

$$\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 2 & 6 & 4 & 3 \end{pmatrix} \quad \sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 3 & 2 & 1 & 4 \end{pmatrix}, \quad \sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 6 & 4 & 2 & 1 \end{pmatrix}$$

We obtain σ^{-1} by interchanging the top and bottom rows of σ and then rearranging:

$$\sigma^{-1} = \begin{pmatrix} 3 & 1 & 5 & 4 & 6 & 2 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 1 & 4 & 3 & 5 \end{pmatrix}$$

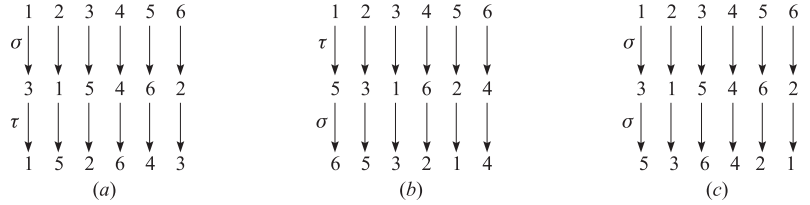


Fig. 12-8

12.13. Let S be the square in the plane $\mathbf{R}^2$ pictured in Fig. 12-9, with its center at the origin 0. Note that the vertices of S are numbered counterclockwise from 1 to 4. (*a*) Define the group G of symmetries of S. (*b*) List the elements of G. (*c*) Find a minimum set of generators of G.

(*a*) A symmetry σ of S is a rigid one-to-one correspondence between S and itself. (Here rigid means that distances between points do not change.) The group G of symmetries of S is the set of all symmetries of S under composition of mappings.

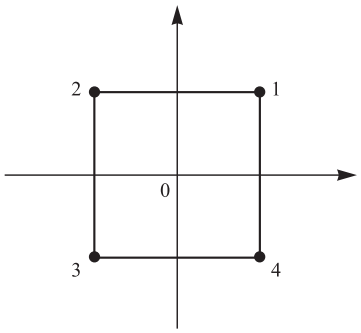


Fig. 12-9

(*b*) There are eight symmetries as follows. For $\alpha = 0°$, $90°$, $180°$, and $270°$, let $\sigma(\alpha)$ be the symmetry obtained by rotating S about its center α degrees, and let $\tau(\alpha)$ be the symmetry obtained by reflecting S about the y axis and then rotating S about its center α degrees. Note that any symmetry σ of S is completely determined by its effect on the vertices of S and hence σ can be represented as a permutation in S_4. Thus:

$$\sigma(0°) = \begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}, \quad \sigma(90°) = \begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}, \quad \sigma(180°) = \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix},$$

$$\sigma(270°) = \begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix}$$

$$\tau(0°) = \begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}, \quad \tau(90°) = \begin{pmatrix}1&2&3&4\\3&2&1&4\end{pmatrix}, \quad \tau(180°) = \begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix},$$

$$\tau(270°) = \begin{pmatrix}1&2&3&4\\1&4&3&2\end{pmatrix}$$

(*c*) Let $a = \sigma(90°)$ and $b = \tau(0°)$. Then a and b form a minimum set of generators of G. Specifically,

$$\sigma(0°) = a^4, \quad \sigma(90°) = a, \quad \sigma(180°) = a^2, \quad \sigma(270°) = a^3$$
$$\tau(0°) = b, \quad \tau(90°) = ba, \quad \tau(180°) = ba^2, \quad \tau(270°) = ba^3$$

and G is not cyclic so it is not generated by one element. (One can show that the relations $a^4 = e$, $b^2 = e$, and $bab = a^{-1}$ completely describe G.)

12.14. Let H and K be groups. (*a*) Define the direct product $G = H \times K$ of H and K. (*b*) What is identity element and the order of $G = H \times K$? (*c*) Describe and find the multiplication table of the group $G = \mathbf{Z}_2 \times \mathbf{Z}_2$.

(*a*) Let $G = H \times K$, the Cartesian product of H and K, with the operation $*$ defined componentwise by

$$(h,k) * (h'k') = (hh', kk')$$

Then G is a group (Problem 12.73), called the *direct product* of H and K.

(*b*) The element $e = (e_H, e_K)$ is the identity element of G, and $|G| = |H|\ |K|$.

(*c*) Since $\mathbf{Z}_2$ has two elements, G has four elements. Let

$$e = (0,0), \quad a = (1,0), \quad b = (0,1), \quad c = (1,1)$$

The multiplication table of G appears in Fig. 12-10. Note that G is abelian since the table is symmetric. Also,

$$a^2 = e, \quad b^2 = e, \quad c^2 = e$$

Thus G is not cyclic, and hence $G \not\approx \mathbf{Z}_4$.

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Fig. 12-10

12.15. Let G be a group and let A be a nonempty set.

(a) Define the meaning of the statement "G acts on A".

(b) Define the stabilizer H_a of an element $a \in A$.

(c) Show that H_a is a subgroup of G.

(a) Let $\text{PERM}(A)$ denote the group of all permutations of A. Let $\Psi: G \to \text{PERM}(A)$ be any homomorphism. Then G is said to *act on* A where each element g in G defines a permutation $g: A \to A$ by

$$g(a) = (\Psi(g))(a)$$

(Frequently, the permuation $g: A \to A$ is given directly and hence the homomorphism Ψ is implicitly defined.)

(b) The stabilizer H_a of $a \in A$ consists of all elements of G which *fix* a, that is,

$$H_a = \{g \in G: g(a) = a\}$$

(c) Since $e(a) = a$, we have $e \in H_a$. Suppose $g,\ g' \in H_a$. Then $(gg')(a) = g(g'(a)) = g(a) = a$; hence $gg' \in H_a$. Also, $g^{-1}(a) = a$ since $g(a) = a$; hence $g^{-1} \in H_a$. Thus H_a is a subgroup of G.

12.16. Let $S = \mathbf{R}^2$, the Cartesian plane. Find the stabilizer H_a of $a = (1, 0)$ in S where G is the following group acting on S:

(a) $G = \mathbf{Z} \times \mathbf{Z}$ and G acts on S by

$$g(x, y) = (x + m, y + n) \qquad \text{where} \qquad g = (m, n)$$

That is, each element g of G is a translation of S.

(b) $G = (\mathbf{R}, +)$ and G acts on S by

$$g(x, y) = (x\ \cos\ g - y\ \sin g,\ x\ \sin\ g + y\ \cos\ g)$$

That is, each element g of G rotates S about the origin by an angle g.

(a) Let $g = (m, n)$. Then

$$g(a) = g(1, 0) = (1 + m, n) = (1, 0) = a$$

if and only if $g = (0, 0)$. Thus H_a consists only of the identity element $(0, 0)$ of G.

(b) Any rotation which is a multiple of 2π fixes a; hence $H_a = \{2\pi r: r \in \mathbf{Z}\}$.

12.17. Prove Theorem 12.6: Let H be a subgroup of a group G. Then the right cosets Ha form a partition of G.

Since $e \in H$, $a = ea \in Ha$; hence every element belongs to a coset. In fact, $a \in Ha$. Now suppose Ha and Hb are not disjoint. Say $c \in Ha \cap Hb$. The proof is complete if we show that $Ha = Hb$.

Since c belongs to both Ha and Hb, we have $c = h_1a$ and $c = h_2b$, where $h_1, h_2 \in H$. Then $h_1a = h_2b$, and so $a = h_1^{-1}h_2b$. Let $x \in Ha$. Then

$$x = h_3a = h_3h_1^{-1}h_2b$$

where $h_3 \in H$. Since H is a subgroup, $h_3h_1^{-1}h_2 \in H$; hence $x \in Hb$. Since x was any element of Ha, we have $Ha \subseteq Hb$. Similarly, $Hb \subseteq Ha$. Both inclusions imply $Ha = Hb$, and the theorem is proved.

12.18. Let H be a finite subgroup of G. Show that H and any coset Ha have the same number of elements.

Let $H = \{h_1, h_2, \ldots, h_k\}$, where H has k elements. Then $Ha = \{h_1a, h_2a, \ldots, h_ka\}$. However, $h_ia = h_ja$ implies $h_i = h_j$; hence the k elements listed in Ha are distinct. Thus H and Ha have the same number of elements.

12.19. Prove Theorem 12.7 (Lagrange): Let H be a subgroup of a finite group G. Then the order of H divides the order of G.

Suppose H has r elements and there are s right cosets; say

$$Ha_1, Ha_2, \ldots, Ha_s$$

By Theorem 12.6, the cosets partition G and by Problem 12.18, each coset has r elements. Therefore G has rs elements, and so the order of H divides the order of G.

12.20. Let G be a group of order p where p is a prime. Find all subgroups of G.

By Lagrange's theorem, the order of a subgroup H of G divides the order of G. Hence $|H| = 1$ or p. Thus $\{e\}$ and G, itself, are the only subgroups of G.

12.21. Let G be a finite group of order n. Show that $a^n = e$ for any element $a \in G$.

Suppose m is the order of $g(a)$. Then $a^m = e$. Also, by Lagrange's theorem m divides n, say $n = mr$. Then

$$a^n = a^{mr} = (a^m)^r = e^r = e$$

12.22. Prove: Every subgroup of a cyclic group G is cyclic.

Since G is cyclic, there is an element a in G such that $G = gp(a)$. Let H be a subgroup of G. If $H = \{e\}$, then $H = gp(e)$ and is cyclic. Otherwise, H contains a nonzero power of a. Since H is a subgroup, it must be closed under inverses and so contains positive powers of a. Let m be the smallest positive power of a such that a^m belongs to H. We claim that $b = a^m$ generates H. Let x be any other element of H; since x belongs to G we have $x = a^n$ for some integer n. Dividing n by m we get a quotient q and a remainder r, i.e.,

$$n = mq + r$$

where $0 \leq r < m$. Then

$$a^n = a^{mq+r} = a^{mq} \cdot a^r = b^q \cdot a^r \qquad \text{so} \qquad a^r = b^{-q}a^n$$

But a^n, $b \in H$. Since H is a subgroup, $b^{-q}a^n \in H$, which means $a^r \in H$. However, m was the smallest positive power of a belonging to H. Therefore $r = 0$. Hence $a^n = b^q$. Thus b generates H, and so H is cyclic.

12.23. Let H be a subgroup and let K be a normal subgroup of a group G. Prove that HK is a subgroup of G.

We must show that $e \in HK$ and that HK is closed under multiplication and inverses. Since H and K are subgroups, $e \in H$ and $e \in K$. Hence $e = e \cdot e$ belongs to HK. Suppose $x, y \in HK$. Then $x = h_1k_1$ and $y = h_2k_2$ where $h_1, h_2 \in H$ and $k_1, k_2 \in K$. Then

$$xy = h_1k_1h_2k_2 = h_1h_2(h_2^{-1}k_1h_2)k_2$$

Since K is normal, $h_2^{-1}k_1h_2 \in K$; and since H and K are subgroups, $h_1h_2 \in H$ and $(h_2^{-1}k_2h_2)k_2 \in K$. Thus $xy \in HK$, and so HK is closed under multiplication. We also have that

$$x^{-1} = (h_1k_1)^{-1} = k_1^{-1}h_1^{-1} = h_1^{-1}(h_1k_1^{-1}h_1^{-1})$$

Since K is a normal subgroup $h_1k_1^{-1}h_1^{-1}$ belongs to K. Also h_1^{-1} belongs to H. Therefore $x^{-1} \in HK$, and hence HK, is closed under inverses. Consequently, HK is a subgroup.

12.24. Prove Theorem 12.8: Let H be a normal subgroup of a group G. Then the cosets of H in G form a group under coset multiplication defined by $(aH)(bH) = abH$.

Coset multiplication is well-defined, since

$$(aH)(bH) = a(Hb)H = a(bH)H = ab(HH) = abH$$

(Here we have used the fact that H is normal, so $Hb = bH$, and, from Problem 12.61, that $HH = H$.) Associativity of coset multiplication follows from the fact that associativity holds in G. H is the identity element of G/H, since

$$(aH)H = a(HH) = aH \qquad \text{and} \qquad H(aH) = (Ha)H = (aH)H = aH$$

Lastly, $a^{-1}H$ is the inverse of aH since

$$(a^{-1}H)(aH) = a^{-1}aH = eH = H \qquad \text{and} \qquad (aH)(a^{-1}H) = aa^{-1}H = eH = H$$

Thus G/H is a group under coset multiplication.

12.25. Suppose $f: G \to G'$ is a group homomorphism. Prove: (*a*) $f(e) = e'$; (*b*) $f(a^{-1}) = f(a)^{-1}$.

(*a*) Since $e = ee$ and f is a homomorphism, we have

$$f(e) = f(ee) = f(e)f(e)$$

Multiplying both sides by $f(e)^{-1}$ gives us our result.

(*b*) Using part (*a*) and that $aa^{-1} = a^{-1}a = e$, we have

$$e' = f(e) = f(aa^{-1}) = f(a)f(a^{-1}) \qquad \text{and} \qquad e' = f(e) = f(a^{-1}a) = f(a^{-1})f(a)$$

Hence $f(a^{-1})$ is the inverse of $f(a)$; that is, $f(a^{-1}) = f(a)^{-1}$.

12.26. Prove Theorem 12.9: Let $f: G \to G'$ be a homomorphism with kernel K. Then K is a normal subgroup of G, and G/K is isomorphic to the image of f. (Compare with Problem 12.8, the analogous theorem for semigroups.)

Proof that K is normal: By Problem 12.19, $f(e) = e'$, so $e \in K$. Now suppose $a, b \in K$ and $g \in G$. Then $f(a) = e'$ and $f(b) = e'$. Hence

$$f(ab) = f(a)f(b) = e'e' = e'$$
$$f(a^{-1}) = f(a)^{-1} = e'^{-1} = e'$$
$$f(gag^{-1}) = f(g)f(a)f(g^{-1}) = f(g)e'f(g)^{-1} = e'$$

Hence ab, a^{-1}, and gag^{-1} belong to K, so K is a normal subgroup.

Proof that $G/K \simeq H$, where H is the image of f: *Let $\phi: G/K \to H$ be defined by*

$$\phi(Ka) = f(a)$$

We show that ϕ is well-defined, i.e., if $Ka = Kb$ then $\phi(Ka) = \phi(Kb)$. Suppose $Ka = Kb$. Then $ab^{-1} \in K$ (Problem 12.61). Then $f(ab^{-1}) = e'$, and so

$$f(a)f(b)^{-1} = f(a)f(b^{-1}) = f(ab^{-1}) = e'$$

Hence $f(a) = f(b)$, and so $\phi(Ka) = \phi(Kb)$. Thus ϕ is well-defined. We next show that ϕ is a homomorphism:

$$\phi(KaKb) = \phi(Kab) = f(ab) = f(a)f(b) = \phi(Ka)\phi(Kb)$$

Thus ϕ is a homomorphism. We next show that ϕ is one-to-one. Suppose $\phi(Ka) = \phi(Kb)$. Then

$$f(a) = f(b) \quad \text{or} \quad f(a)f(b)^{-1} = e' \quad \text{or} \quad f(a)f(b^{-1}) = e' \quad \text{or} \quad f(ab^{-1}) = e'$$

Thus $ab^{-1} \in K$, and by Problem 12.61 we have $Ka = Kb$. Thus ϕ is one-to-one. We next show that ϕ is onto. Let $h \in H$. Since H is the image of f, there exists $a \in G$ such that $f(a) = h$. Thus $\phi(Ka) = f(a) = h$, and so ϕ is onto. Consequently $G/K \cong H$ and the theorem is proved.

12.27. Let G be a group and let $g \in G$. Define a function $\hat{g}: G \to G$ by $\hat{g}(x) = gxg^{-1}$. Show that $\hat{g}$ is an isomorphism of G onto G, i.e., show that:

$$(a)\ \hat{g} \text{ is a homomorphism, } (b)\ \hat{g} \text{ is one-to-one, } (c)\ \hat{g} \text{ is onto.}$$

(*a*) We have $\hat{g}(xy) = gxyg^{-1} = (gxg^{-1})(gyg^{-1}) = \hat{g}(x)\hat{g}(y)$. Hence g is a homomorphism.

(*b*) Suppose $\hat{g}(x) = \hat{g}(y)$. Then $gxg^{-1} = gyg^{-1}$. By cancelation, $x = y$. Thus $\hat{g}$ is one-to-one.

(*c*) Suppose $z \in G$. Then $\hat{g}(g^{-1}zg) = gg^{-1}zgg^{-1} = z$. Hence $\hat{g}$ is onto.

RINGS, INTEGRAL DOMAINS, FIELDS

12.28. Consider the ring $\mathbf{Z}_{10} = \{0, 1, 2, \ldots, 9\}$ of integers modulo 10.

(*a*) Find the units of $\mathbf{Z}_{10}$.

(*b*) Find -3, -8, and 3^{-1}.

(*c*) Let $f(x) = 2x^2 + 4x + 4$. Find the roots of $f(x)$ over $\mathbf{Z}_{10}$.

(*a*) By Problem 12.83 those integers relatively prime to the modulus $m = 10$ are the units in $\mathbf{Z}_{10}$. Hence the units are 1, 3, 7, and 9.

(*b*) By $-a$ in a ring R we mean that element such that $a + (-a) = (-a) + a = 0$. Hence $-3 = 7$ since $3 + 7 = 7 + 3 = 0$ in $\mathbf{Z}_{10}$. Similarly $-8 = 2$. By a^{-1} in a ring R we mean that element such that $a \cdot a^{-1} = a^{-1} \cdot a = 1$. Hence $3^{-1} = 7$ since $3 \cdot 7 = 7 \cdot 3 = 1$ in $\mathbf{Z}_{10}$.

(*c*) Substitute each of the ten elements of $\mathbf{Z}_{10}$ into $f(x)$ to see which elements yield 0. We have:

$$f(0) = 4, \quad f(2) = 0, \quad f(4) = 2, \quad f(6) = 0, \quad f(8) = 4$$
$$f(1) = 0, \quad f(3) = 4, \quad f(5) = 4, \quad f(7) = 0, \quad f(9) = 2$$

Thus the roots are 1, 2, 6 and 7. (This example shows that a polynomial of degree n can have more than n roots over an arbitrary ring. This cannot happen if the ring is a field.)

12.29. Prove that in a ring R: (i) $a \cdot 0 = 0 \cdot a = 0$; (ii) $a(-b) = (-a)b = -ab$; (iii) $(-1)a = -a$ (when R has an identity element 1).

(i) Since $0 = 0 + 0$, we have

$$a \cdot 0 = a(0 + 0) = a \cdot 0 + a \cdot 0$$

Adding $-(a \cdot 0)$ to both sides yields $0 = a \cdot 0$. Similarly $0 \cdot a = 0$.

(ii) Using $b + (-b) = (-b) + b = 0$, we have

$$ab + a(-b) = a(b + (-b)) = a \cdot 0 = 0$$
$$a(-b) + ab = a((-b) + b) = a \cdot 0 = 0$$

Hence $a(-b)$ is the negative of ab; that is, $a(-b) = -ab$. Similarly, $(-a)b = -ab$.

(iii) We have

$$a + (-1)a = 1 \cdot a + (-1)a = (1 + (-1))a = 0 \cdot a = 0$$
$$(-1)a + a = (-1)a + 1 \cdot a = ((-1) + 1)a = 0 \cdot a = 0$$

Hence $(-1)a$ is the negative of a; that is, $(-1)a = -a$.

12.30. In an integral domain D, show that if $ab = ac$ with $a \neq 0$ then $b = c$.

Since $ab = ac$ we have

$$ab - ac = 0 \qquad \text{and so} \qquad a(b - c) = 0$$

Since $a \neq 0$, we must have $b - c = 0$, since D has no zero divisors. Hence $b = c$.

12.31. Suppose J and K are ideals in a ring R. Prove that $J \cap K$ is an ideal in R.

Since J and K are ideals, $0 \in J$ and $0 \in K$. Hence $0 \in J \cap K$. Now let $a, b \in J \cap K$ and let $r \in R$. Then $a, b \in J$ and $a, b \in K$. Since J and K are ideals,

$$a - b,\ ra,\ ar \in J \qquad \text{and} \qquad a - b,\ ra,\ ar \in K$$

Hence $a - b$, ra, $ar \in J \cap K$. Therefore $J \cap K$ is an ideal.

12.32. Let J be an ideal in a ring R with an identity element 1. Prove: (*a*) If $1 \in J$ then $J = R$. (*b*) If any unit $u \in J$ then $J = R$.

(*a*) If $1 \in J$ then for any $r \in R$ we have $r \cdot 1 \in J$ or $r \in J$. Hence $J = R$.

(*b*) If $u \in J$ then $u^{-1} \cdot u \in J$ or $1 \in J$. Hence $J = R$ by part (*a*).

12.33. Prove: (*a*) A finite integral domain D is a field.
(*b*) $\mathbf{Z}_p$ is a field where p is a prime number.
(*c*) (Fermat) If p is prime, then $a^p \equiv a \pmod{p}$ for any integer a.

(*a*) Suppose D has n elements, say $D = \{a_1, a_3, \ldots, a_n\}$. Let a be any nonzero element of D. Consider the n elements

$$aa_1, \quad aa_2, \quad \ldots, \quad aa_n$$

Since $a \neq 0$, we have $aa_i = aa_j$ implies $a_i = a_j$ (Problem 12.30). Thus the n elements above are distinct, and so they must be a rearrangement of the elements of D. One of them, say aa_k, must equal the identity element 1 of D; that is, $aa_k = 1$. Thus a_k is the inverse of a. Since a was any nonzero element of D, we have that D is a field.

(*b*) Recall $\mathbf{Z}_p = \{0, 1, 2, \ldots, p - 1\}$. We show that $\mathbf{Z}_p$ has no zero divisors. Suppose $a * b = 0$ in $\mathbf{Z}_p$; that is, $ab \equiv 0 \pmod{p}$. Then p divides ab. Since p is prime, p divides a or p divides b. Thus $a \equiv 0 \pmod{p}$ or $b \equiv 0 \pmod{p}$; that is, $a = 0$ or $b = 0$ in $\mathbf{Z}_p$. Accordingly, $\mathbf{Z}_p$ has no zero divisors and hence $\mathbf{Z}_p$ is an integral domain. By part (*a*), $\mathbf{Z}_p$ is a field.

(*c*) If p divides a, then $a \equiv 0 \pmod{p}$ and so $a^p \equiv a \equiv 0 \pmod{p}$. Suppose p does not divide a, then a may be viewed as a nonzero element of $\mathbf{Z}_p$. Since $\mathbf{Z}_p$ is a field, its nonzero elements form a group G under multiplication of order $p - 1$. By Problem 12.21, $a^{p-1} = 1$ in $\mathbf{Z}_p$. In other words, $a^{p-1} \equiv 1 \pmod{p}$. Multiplying by a gives $a^p \equiv a \pmod{p}$, and the theorem is proved.

POLYNOMIALS OVER A FIELD

12.34. Suppose $f(t) = t^3 - 2t^2 - 6t - 3$. Find the roots of $f(t)$ assuming $f(t)$ has an integer root.

The integer roots of $f(t)$ must be among $\pm 1, \pm 3$. Note $f(1) \neq 0$. Using synthetic division, or dividing by $t + 1$, we get:

$$\begin{array}{r|rrrrrr} -1 & 1 & - & 2 & - & 6 & - & 3 \\ & & - & 1 & + & 3 & + & 3 \\ \hline & 1 & - & 3 & - & 3 & + & 0 \end{array}$$

Therefore $t = -1$ is a root and $f(t) = (t + 1)(t^2 - 3t - 3)$. We can now use the quadratic formula on $t^2 - 3t - 3$ to obtain the following three roots of $f(t)$:

$$t = -1, \qquad t = (3 + \sqrt{21})/2, \qquad t = (3 - \sqrt{21})/2$$

12.35. Suppose $f(t) = 2t^3 - 3t^2 - 6t - 2$. Find all the roots of $f(t)$ knowing that $f(t)$ has a rational root.

The rational roots of $f(t)$ must be among $\pm 1, \pm 2, \pm \frac{1}{2}$. Testing each possible root, we get, by synthetic division (or dividing by $2t + 1$),

$$\begin{array}{r|rrrrrr} -\frac{1}{2} & 2 & - & 3 & - & 6 & - & 2 \\ & & - & 1 & + & 2 & + & 2 \\ \hline & 2 & - & 4 & - & 4 & + & 0 \end{array}$$

Therefore $t = -\frac{1}{2}$ is a root and

$$f(t) = (t + \tfrac{1}{2})(2t^2 - 4t - 4) = (2t + 1)(t^2 - 2t - 2)$$

We can now use the quadratic formula on $t^2 - 2t - 2$ to obtain the following three roots of $f(t)$:

$$t = -\tfrac{1}{2}, \qquad t = 1 + \sqrt{3}, \qquad t = 1 - \sqrt{3}$$

12.36. Let $f(t) = t^4 - 3t^3 + 3t^2 + 3t - 20$. Find all the roots of $f(t)$ given that $t = 1 + 2i$ is a root.

Since $1 + 2i$ is a root, then $1 - 2i$ is a root and $c(t) = t^2 - 2t + 5$ is a factor of $f(t)$. Dividing $f(t)$ by $c(t)$ we get

$$f(t) = (t^2 - 2t + 5)(t^2 - t - 4)$$

The quadratic formula with $t^2 - t - 4$ gives us the other roots of $f(t)$. That is, the four roots of $f(t)$ follow:

$$t = 1 + 2i, \qquad t = 1 - 2i, \qquad t = (1 + \sqrt{17})/2, \qquad t = (1 - \sqrt{17})/2$$

12.37. Let $K = \mathbf{Z}_8$. Find all roots of $f(t) = t^2 + 6t$.

Here $\mathbf{Z}_8 = \{0, 1, 2, \ldots, 7\}$. Substitute each element of $\mathbf{Z}_8$ into $f(t)$ to obtain:

$$f(0) = 0, \qquad f(2) = 0, \qquad f(4) = 0, \qquad f(6) = 0$$

Then $f(t)$ has four roots, $t = 0, 2, 4, 6$. (Theorem 12.21 does not hold here since K is not a field.)

12.38. Suppose $f(t)$ is a real polynomial with odd degree n.

(a) Show algebraically that $f(t)$ has a real root.

(b) Show geometrically, that $f(t)$ has a real root.

(a) The complex roots of $f(t)$ come in pairs. Since $f(t)$ has an odd number n of roots (counting multiplicity), $f(t)$ must have at least one real root.

(b) Suppose the leading coefficient of $f(t)$ is positive [otherwise, multiply $f(t)$ by -1]. Since $\deg(f) = n$ where n is odd, we have

$$\lim_{t\to\infty} f(t) = +\infty \qquad \text{and} \qquad \lim_{t\to-\infty} f(t) = -\infty$$

Thus the graph of $f(t)$ must cross the t axis in at least one point as shown in Fig. 12-11.

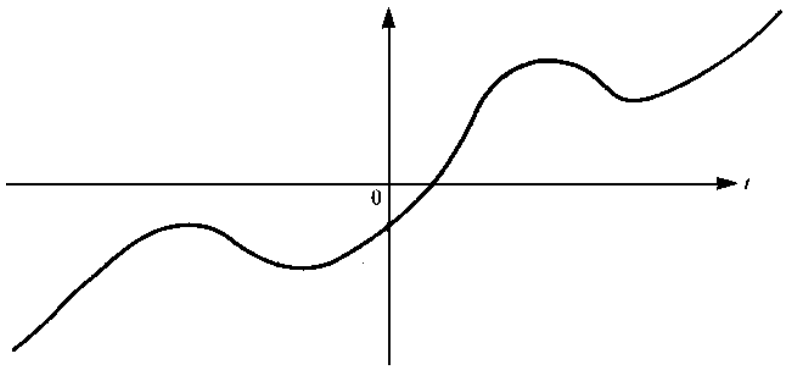


Fig. 12-11

12.39. Prove Theorem 12.15 (Euclidean Division Algorithm): Let $f(t)$ and $g(t)$ be polynomials over a field K with $g(t) \neq 0$. Then there exist polynomials $q(t)$ and $r(t)$ such that

$$f(t) = q(t)g(t) + r(t)$$

where either $r(t) \equiv 0$ or $\deg(r) < \deg(g)$.

If $f(t) = 0$ or if $\deg(f) < \deg(g)$, then we have the required representation $f(t) = 0g(t) + f(t)$. Now suppose $\deg(f) \geq \deg(g)$, say $f(t) = a_n t^n + \cdots + a_1 t + a_0$ and $g(t) = b_m t^m + \cdots + b_1 t + b_0$ where $a_n, b_m \neq 0$ and $n \geq m$. We form the polynomial

$$f_1(t) = f(t) - \frac{a_n}{b_m} t^{n-m} g(t) \tag{1}$$

(This is the first subtraction step in "long division.") Then $\deg(f_1) < \deg(f)$. By induction, there exist polynomials $q_1(t)$ and $r(t)$ such that $f_1(t) = q_1(t)g(t) + r(t)$ where either $r(t) \equiv 0$ or $\deg(r) < \deg(g)$. Substituting this into (1) and solving for $f(t)$, we get

$$f(t) = \left(q_1(t) + \frac{a_n}{b_m} t^{n-m}\right) g(t) + r(t)$$

which is the desired representation.

12.40. Prove Theorem 12.18: Suppose $f(t)$ is a polynomial over a field K, and $\deg(f) = n$. Then $f(t)$ has at most n roots.

The proof is by induction on n. If $n = 1$, then $f(t) = at + b$ and $f(t)$ has the unique root $t = -b/a$. Suppose $n > 1$. If $f(t)$ has no roots, then the theorem is true. Suppose $a \in K$ is a root of $f(t)$. Then

$$f(t) = (t - a)g(t) \tag{1}$$

where $\deg(g) = n - 1$. We claim that any other root of $f(t)$ must also be a root of $g(t)$. Suppose $b \neq a$ is another root of $f(t)$. Substituting $t = b$ in (1) yields $0 = f(b) = (b - a)g(b)$. Since K has no zero divisors, and $b - a \neq 0$, we must have $g(b) = 0$. By induction, $g(t)$ has at most $n - 1$ roots. Thus $f(t)$ has at most $n - 1$ roots other than a. Thus $f(t)$ has at most n roots.

12.41. Prove Theorem 12.19: Suppose a rational number p/q (reduced to lowest terms) is a root of the polynomial

$$f(t) = a_n t^n + \cdots + a_1 t + a_0$$

where all the coefficients $a_n, \ldots, a_1, a_0$ are integers. Then p divides the constant term a_0 and q divides the leading coefficients a_n. In particular, if $c = p/q$ is an integer, then c divides the constant term a_0.

Substitute $t = p/q$ into $f(t) = 0$ to obtain $a_n(p/q)^n + \cdots + a_1(p/q) + a_0 = 0$. Multiply both sides of the equation by q^n to obtain

$$a_n p^n + a_{n-1} p^{n-1} q + a_{n-2} p^{n-2} q^2 + \cdots + a_1 p q^{n-1} + a_0 q^n = 0 \tag{1}$$

Since p divides all of the first n terms of (1), p must divide the last term $a_0 q^n$. Assuming p and q are relatively prime, p divides a_0. Similarly, q divides the last n terms of (1), hence q divides the first term $a_n p^n$. Since p and q are relatively prime, q divides a_n.

12.42. Prove Theorem 12.20: The ring $K[t]$ of polynomials over a field K is a principal ideal domain (PID). If J is an ideal in $K[t]$, then there exists a unique monic polynomial d which generates J, that is, every polynomial f in J is a multiple of d.

Let d be a polynomial of lowest degree in J. Since we can multiply d by a nonzero scalar and still remain in J, we can assume without loss in generality that d is a monic polynomial. Now suppose $f \in J$. By the division algorithm there exist polynomials q and r such that $f = qd + r$ where either $r = 0$ or $\deg(r) < \deg(d)$. Now $f, d \in J$ implies $qd \in J$ and hence $r = f - qd \in J$. But d is a polynomial of lowest degree in J. Accordingly, $r = 0$ and $f = qd$, that is, d divides f. It remains to show that d is unique. If d' is another monic polynomial which generates J, then d divides d' and d' divides d. This implies that $d = d'$, because d and d' are monic. Thus the theorem is proved.

12.43. Prove theorem 12.21: Let f and g be polynomials in $K[t]$, not both the zero polynomial. Then there exists a unique monic polynomial d such that: (i) d divides both f and g. (ii) If d' divides f and g, then d' divides d.

The set $I = \{mf + ng : m, n \in K[t]\}$ is an ideal. Let d be the monic polynomial which generates I. Note $f, g \in I$; hence d divides f and g. Now suppose d' divides f and g. Let J be the ideal generated by d'. Then $f, g \in J$ and hence $I \subseteq J$. Accordingly, $d \in J$ and so d' divides d as claimed. It remains to show that d is unique. If d_1 is another (monic) greatest common divisor of f and g, then d divides d_1 and d_1 divides d. This implies that $d = d_1$ because d and d_1 are monic. Thus the theorem is proved.

12.44. Prove Corollary 12.22: Let d be the greatest common divisor of f and g. Then there exist polynomials m and n such that $d = mf + ng$. In particular, if f and g are relatively prime, then there exist polynomials m and n such that $mf + ng = 1$.

From the proof of Theorem 12.21 in Problem 12.43, the greatest common divisor d generates the ideal $I = \{mf + ng : m, n \in K[t]$. Thus there exist polynomials m and n such that $d = mf + ng$.

12.45. Prove Lemma 12.23: Suppose $p \in K[t]$ is irreducible. If p divides the product fg of polynomials $f, g \in K[t]$, then p divides f or p divides g. More generally, if p divides the product $f_1 f_2 \cdots f_n$ of n polynomials, then p divides one of them.

Suppose p divides fg but not f. Since p is irreducible, the polynomials f and p must then be relatively prime. Thus there exist polynomials $m, n \in K[t]$ such that $mf + np = 1$. Multiplying this equation by g, we obtain $mfg + npg = g$. But p divides fg and so mfg, and p divides npg; hence p divides the sum $g = mfg + npg$.

Now suppose p divides $f_1 f_2 \cdots f_n$. If p divides f_1, then we are through. If not, then by the above result p divides the product $f_2 \cdots f_n$. By induction on n, p divides one of the polynomials $f_2, \cdots, f_n$. Thus the lemma is proved.

12.46. Prove Theorem 12.24 (Unique Factorization Theorem): Let f be a nonzero polynomial in $K[t]$. Then f can be written uniquely (except for order) as a product $f = kp_1 p_2 \cdots p_n$ where $k \in K$ and the p's are monic irreducible polynomials in $K[t]$.

We prove the existence of such a product first. If f is irreducible or if $f \in K$, then such a product clearly exists. On the other hand, suppose $f = gh$ where g and h are nonscalars. Then g and h have degrees less than that of f. By induction, we can assume $g = k_1 g_1 g_2 \cdots g_r$, and $h = k_2 h_1 h_2 \cdots h_s$ where $k_1, k_2 \in K$ and the g_i and h_j are monic irreducible polynomials. Accordingly, $f = (k_1 k_2) g_1 g_2 \cdots g_r h_1 h_2 \cdots h_s$ is our desired representation.

We next prove uniqueness (except for order) of such a product for f. Suppose

$$f = kp_1 p_1 \cdots p_n = k' q_1 q_2 \cdots q_m \qquad \text{where} \qquad k, k' \in K$$

and the $p_1, \cdots, p_n, q_1, \cdots, q_m$ are monic irreducible polynomials. Now p_1 divides $k' q_1 \cdots q_m$. Since p_1 is irreducible it must divide one of the q's by Lemma 12.23. Say p_1 divides q_1. Since p_1 and q_1 are both irreducible and monic, $p_1 = q_1$. Accordingly, $kp_2 \cdots p_n = k' q_2 \cdots q_m$. By induction, we have that $n = m$ and $p_2 = q_2, \cdots, p_n = q_m$ for some rearrangement of the q_i. We also have that $k = k'$. Thus the theorem is proved.

12.47. Prove Theorem 12.25: Suppose $f(t)$ is a polynomial over the real field $\mathbf{R}$, and suppose the complex number $z = a + bi$, $b \neq 0$, is a root of $f(t)$. Then the complex conjugate $\bar{z} = a - bi$ is also a root of $f(t)$. Hence

$$c(t) = (t - z)(t - \bar{z}) = t^2 - 2at + a^2 + b^2$$

is a factor of $f(t)$.

Since $\deg(c) = 2$, there exist $q(t)$ and real numbers M and N such that

$$f(t) = c(t)q(t) + Mt + N \tag{1}$$

Since $z = a + bi$ is a root of $f(t)$ and $c(t)$, we have, by substituting $t = a + bi$ in (1),

$$f(z) = c(z)q(z) + M(z) + n \qquad \text{or} \qquad 0 = 0q(z) + M(z) + N \qquad \text{or} \qquad M(a + bi) + N = 0$$

Thus $Ma + N = 0$ and $Mb = 0$. Since $b \neq 0$, we must have $M = 0$. Then $0 + N = 0$ or $N = 0$. Accordingly, $f(t) = c(t)q(t)$ and $\bar{z} = a - bi$ is a root of $f(t)$.

Supplementary Problems

OPERATIONS AND SEMIGROUPS

12.48. Let $*$ be the operation on the set $\mathbf{R}$ of real numbers defined by $a * b = a + b + 2ab$.

(*a*) Find $2 * 3$, $3 * (-5)$, and $7 * (1/2)$.

(*b*) Is $(\mathbf{R}, *)$ a semigroup? Is it commutative?

(*c*) Find the identity element.

(*d*) Which elements have inverses and what are they?

12.49. Let A be a nonempty set with the operation $*$ defined by $a * b = a$, and assume A has more than one element. (*a*) Is A a semigroup? (*b*) Is A commutative? (*c*) Does A have an identity element? (*d*) Which elements, if any, have inverses and what are they?

12.50. Let $A = \{a, b\}$. Find the number of operations on A, and exhibit one which is neither associative nor commutative.

12.51. Let $A = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}$, i.e., the multiples of 3. Is A closed under: (*a*) addition, (*b*) multiplication, (*c*) subtraction, (*d*) division (except by 0)?

12.52. Find a set A of three numbers which is closed under: (*a*) multiplication, (*b*) addition.

12.53. Let S be an infinite set. Let A be the collection of finite subsets of S and let B be the collection of infinite subsets of S.

(*a*) Is A closed under: (i) union; (ii) intersection, (iii) complements?

(*b*) Is B closed under: (i) union, (ii) intersection, (iii) complements?

12.54. Let $S = \mathbf{Q} \times \mathbf{Q}$, the set of ordered pairs of rational numbers, with the operation $*$ defined by

$$(a, b) * (x, y) = (ax, ay + b)$$

(*a*) Find $(3, 4) * (1, 2)$ and $(-1, 3) * (5, 2)$.

(*b*) Is S a semigroup? Is it commutative?

(*c*) Find the identity element of S.

(*d*) Which elements, if any, have inverses and what are they?

12.55. Let $S = \mathbf{N} \times \mathbf{N}$, the set of ordered pairs of positive integers, with the operation $*$ defined by

$$(a, b) * (c, d) = (ad + bc, bd)$$

(*a*) Find $(3, 4) * (1, 5)$ and $(2, 1) * (4, 7)$.

(*b*) Show that $*$ is associative. [Hence S is a semigroup.]

(*c*) Define $f: (S, *) \to (\mathbf{Q}, +)$ by $f(a, b) = a/b$. Show that f is a homomorphism.

(*d*) Find the congruence relation $\sim$ in S determined by the homomorphism f.

(*e*) Describe $S/\sim$. Does $S/\sim$ have an identity element? Does it have inverses?

GROUPS

12.56. Consider $\mathbf{Z}_{20} = \{0, 1, \ldots, 19\}$ under addition modulo 20. Let H be the subgroup generated by 5.

(*a*) Find the elements and order of H. (*b*) Find the cosets of H in $\mathbf{Z}_{20}$.

12.57. Consider $G = \{1, 5, 7, 11, 13, 17\}$ under multiplication modulo 18.

(*a*) Construct the multiplication table of G.

(*b*) Find 5^{-1}, 7^{-1}, and 17^{-1}.

(*c*) Find the order and group generated by: (i) 5, (ii) 13.

(*d*) Is G cyclic?

12.58. Consider $G = \{1, 5, 7, 11\}$ under multiplication modulo 12. (*a*) Find the order of each element. (*b*) Is G cyclic? (*c*) Find all subgroups.

12.59. Consider the symmetric group S_4. Let

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} \quad \text{and} \quad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$$

(*a*) Find $\alpha\beta$, $\beta\alpha$, α^2, and α^{-1}.

(*b*) Find the orders of α, β, and $\alpha\beta$.

12.60. Prove the following results for a group G.

(*a*) The identity element e is unique.

(*b*) Each a in G has a unique inverse a^{-1}.

(*c*) $(a^{-1})^{-1} = a$, $(ab)^{-1} = b^{-1}a^{-1}$ and, more generally, $(a_1a_2 \cdots a_k)^{-1} = a_k^{-1} \cdots a_2^{-1}a_1^{-1}$.

(*d*) $ab = ac$ implies $b = c$, and $ba = ca$ implies $b = c$.

(*e*) For any integers r and s, we have $a^r a^s = a^{r+s}$ and $(a^r)^s = a^{rs}$.

(*f*) G is abelian if and only if $(ab)^2 = a^2b^2$ for all $a, b \in G$.

12.61. Let H be a subgroup of G. Prove: (*a*) $H = Ha$ if and only if $a \in H$. (*b*) $Ha = Hb$ if and only if $ab^{-1} \in H$. (*c*) $HH = H$.

12.62. Prove Proposition 12.5: A subset H of a group G is a subgroup of G if: (*a*) $e \in H$, and (*b*) for all $a, b \in H$, we have ab, $a^{-1} \in H$.

12.63. Let G be a group.

(*a*) Prove that the intersection of any number of subgroups of G is a subgroup of G.

(*b*) Suppose A is a subset of G. Prove $gp(A)$ is equal to the intersection of all subgroups of G containing A.

(*c*) Prove that the intersection of any number of normal subgroups of G is a normal subgroup of G.

12.64. Suppose G is an abelian group. Show that any factor group G/H is also abelian.

12.65. Suppose $|G| = p$, where p is a prime. Prove: (*a*) G has no subgroups except G and $\{e\}$. (*b*) G is cyclic and every element $a \neq e$ generates G.

12.66. Show that $G = \{1, -1, i, -i\}$ is a group under multiplication, and show that $G \simeq \mathbf{Z}_4$ by giving an explicit isomorphism $f: G \to \mathbf{Z}_4$.

12.67. Let H be a subgroup of G with only two right cosets. Show that H is normal.

12.68. Let S be the regular polygon with n sides, and let G be the group of symmetries of S. (*a*) Find the order of G. (*b*) Show that G is generated by two elements a and b such that $a^n = e$, $b^2 = e$, and $b^{-1}ab = a^{-1}$. (G is called the *dihedral group*.)

12.69. Suppose a group G acts on a set S, say by the homomorphism $\Psi: G \to \text{PERM}(S)$.

(*a*) Prove that, for any $s \in S$: (i) $e(s) = s$, and (ii) $(gg')(s) = g(g'(s))$ where $g, g' \in G$.

(*b*) The *orbit* G_s of any $s \in S$ is defined by $G_s = \{g(s): g \in G\}$. Show that the orbits form a partition of S.

(*c*) Show that $|G_s| = [G: H_s]$, the number of cosets of the stabilizer H_s of s in G. [Recall $H_s = \{g \in G: g(s) = s\}$.]

12.70. Let G be an abelian group and let n be a fixed positive integer. Show that the function $f: G \to G$ defined by $f(a) = a^n$ is a homomorphism.

12.71. Let G be the multiplicative group of complex numbers z such that $|z| = 1$, and let $\mathbf{R}$ be the additive group of real numbers. Prove $G \simeq \mathbf{R}/\mathbf{Z}$.

12.72. Suppose H and N are subgroups of G with N normal. Show that: (a) HN is a subgroup of G. (b) $H \cap N$ is a normal subgroup of H. (c) $H/(H \cap N) \simeq HN/N$.

12.73. Let H and K be groups. Let G be the product set $H \times K$ with the operation

$$(h, k) * (h', k') = (hh', kk')$$

(a) Show that G is a group (called the *direct product* of H and K).

(b) Let $H' = H \times \{e\}$. Show that: (i) $H' \cong H$; (ii) H' is a normal subgroup of G; (iii) $G/H' \cong K$.

RINGS

12.74. Consider the ring $\mathbf{Z}_{12} = \{0, 1, \ldots, 11\}$ of integers modulo 12.

(a) Find the units of $\mathbf{Z}_{12}$.

(b) Find the roots of $f(x) = x^2 + 4x + 4$ over $\mathbf{Z}_{12}$.

(c) Find the associates of 2.

12.75. Consider the ring $\mathbf{Z}_{30} = \{0, 1, \ldots, 29\}$ of integers modulo 30.

(a) Find -2, -7 and -11. (b) Find 7^{-1}, 11^{-1} and 26^{-1}.

12.76. Show that in a ring R:

(a) $(-a)(-b) = ab$; (b) $(-1)(-1) = 1$, if R has an identity element 1.

12.77. Suppose $a^2 = a$ for every $a \in R$. (Such a ring is called a *Boolean ring*). Prove that R is commutative.

12.78. Let R be a ring with an identity element 1. We make R into another ring R' by defining

$$a \oplus b = a + b + 1 \qquad \text{and} \qquad a * b = ab + a + b$$

(a) Verify that R' is a ring. (b) Determine the 0-element and the 1-element of R'.

12.79. Let G be any (additive) abelian group. Define a multiplication in G by $a \cdot b = 0$ for every $a, b \in G$. Show that this makes G into a ring.

12.80. Let J and K be ideals in a ring R. Prove that $J + K$ and $J \cap K$ are also ideals.

12.81. Let R be a ring with an identity element. Show that $(a) = \{ra: r \in R\}$ is the smallest ideal containing a.

12.82. Show that R and $\{0\}$ are ideals of any ring R.

12.83. Prove:

(a) The units of a ring R form a group under multiplication.

(b) The units in $\mathbf{Z}_m$ are those integers which are relatively prime to m.

12.84. For any positive integer m, verify that $m\mathbf{Z} = \{rm: r \in \mathbf{Z}\}$ is a ring. Show that $2\mathbf{Z}$ and $3\mathbf{Z}$ are not isomorphic.

12.85. Prove Theorem 12.10: Let J be an ideal in a ring R. Then the cosets $\{a + J : a \in R\}$ form a ring under the coset operations

$$(a + J) + (b + J) = a + b + J \qquad \text{and} \qquad (a + J)(b + J) = ab + J$$

12.86. Prove Theorem 12.11: Let $f: R \to R'$ be a ring homomorphism with kernel K. Then K is an ideal in R, and the quotient ring R/K is isomorphic to $f(R)$.

12.87. Let J be an ideal in a ring R. Consider the (canonical) mapping $f: R \to R/J$ defined by $f(a) = a + J$. Show that: (*a*) f is a ring homomorphism; (*b*) f is an onto mapping.

12.88. Suppose J is an ideal in a ring R. Show that:

(*a*) If R is commutative, then R/J is commutative.

(*b*) If R has a unity element 1 and $1 \notin J$, then $1 + R$ is a unity element for R/J.

INTEGRAL DOMAINS AND FIELDS

12.89. Prove that if $x^2 = 1$ in an integral domain D, then $x = -1$ or $x = 1$.

12.90. Let $R \neq \{0\}$ be a finite commutative ring with no zero divisors. Show that R is an integral domain, i.e., that R has an identity element 1.

12.91. Prove that $F = \{a + b\sqrt{2} : a, b \text{ rational}\}$ is a field.

12.92. Prove that $F = \{a + b\sqrt{2} : a, b \text{ integers}\}$ is an integral domain but not a field.

12.93. A complex number $a + bi$ where a, b are integers is called a *Gaussian integer*. Show that the set G of Gaussian integers is an integral domain. Also show that the units are ± 1, $\pm i$.

12.94. Let R be an integral domain and let J be an ideal in R. Prove that the factor ring R/J is an integral domain if and only if J is a prime ideal. (An ideal J is *prime* if $J \neq R$ and if $ab \in J$ implies $a \in J$ or $b \in J$.]

12.95. Let R be a commutative ring with an identity element 1, and let J be an ideal in R. Prove that the factor ring R/J is a field if and only if J is a maximal ideal. (An ideal J is *maximal* if $J \neq R$ and no ideal K lies strictly between J and R, that is, if $J \subseteq K \subseteq R$ then $J = K$ or $K = R$.)

12.96. Let D be the ring of real 2×2 matrices of the form $\begin{bmatrix} a & -b \\ b & a \end{bmatrix}$. Show that D is isomorphic to the complex field $\mathbf{C}$, whence D is a field.

12.97. Show that the only ideal in a field K is $\{0\}$ or K itself.

12.98. Suppose $f: K \to K'$ is a homomorphism from a field K to a field K'. Show that f is an *embedding*; that is, f is one-to-one. [We assume $f(1) \neq 0$.]

12.99. Consider the integral domain $D = \{a + b\sqrt{13} : a, b \text{ integers}\}$. [See Example 12.16(*b*)]. If $\alpha = a + b\sqrt{13}$, we define $N(\alpha) = a^2 - 13b^2$. Prove: (i) $N(\alpha\beta) = N(\alpha)N(\beta)$. (ii) α is a unit if and only if $N(\alpha) = \pm 1$. (iii) Among the units of D are ± 1, $18 \pm 5\sqrt{13}$; and $-18 \pm 5\sqrt{13}$. (iv) The numbers 2, $3 - \sqrt{13}$ and $-3 - \sqrt{13}$ are irreducible.

POLYNOMIALS OVER A FIELD

12.100. Find the roots of $f(t)$ assuming $f(t)$ has an integer root: (*a*) $f(t) = t^3 - t^2 - 11t - 10$; (*b*) $f(t) = t^3 + 2t^2 - 13t - 6$.

12.101. Find the roots of $f(t)$ assuming $f(t)$ has a rational root: (*a*) $f(t) = 2t^3 - 3t^2 - 16t - 7$; (*b*) $f(t) = 2t^3 - t^2 - 9t + 9$.

12.102. Find the roots of $f(t) = t^4 - 5t^3 + 16t^2 - 9t - 13$, given that $t = 2 + 3i$ is a root.

12.103. Find the roots of $f(t) = t^4 - t^3 - 5t^2 + 12t - 10$, given that $t = 1 - i$ is a root.

12.104. For any scalar $a \in K$, define the *evaluation map* $\Psi_a: K[t] \to K$ by $\Psi_a(f(t)) = f(a)$. Show that Ψ_a is a ring homomorphism.

12.105. Prove Proposition 12.14.

12.106. Prove Theorem 12.26.

Answers to Supplementary Problems

12.48. (*a*) 17, −32, 29/2, (*b*) Yes, yes; (*c*) Zero; (*d*) If $a \neq 1/2$, then a has an inverse which is $-a/(1 + 2a)$.

12.49. (*a*) Yes; (*b*) No; (*c*) No; (*d*) It is meaningless to talk about inverses when no identity element exists.

12.50. Sixteen, since there are two choices, *a* or *b*, for each of the four products *aa*, *ab*, *ba*, and *bb*. In Fig. 12-12, $ab \neq ba$. Also, $(aa)b = bb = a$, but $a(ab) = aa = b$.

*	*a*	*b*
a	*b*	*a*
b	*b*	*a*

Fig. 12-12

12.51. (*a*) Yes; (*b*) yes; (*c*) yes; (*d*) no.

12.52. (*a*) $\{1, -1, 0\}$; (*b*) There is no set.

12.53. (*a*) Yes, yes, no; (*b*) Yes, no, no.

12.54. (*a*) $(3, 10)$, $(-5, 1)$; (*b*) yes, no; (*c*) $(1, 0)$; (*d*) The element (a, b) has an inverse if $a \neq 0$, and its inverse is $(1/a, -b/a)$.

12.55. (*a*) $(19, 20)$, $(18/7)$. (*b*) Yes. (*d*) $(a, b) \sim (c, d)$ if $ad = bc$.
(*e*) $S/\sim$ is isomorphic to the positive rational numbers under addition. Thus $S/\sim$ has no identity element and no inverses.

12.56. (*a*) $H = \{0, 5, 10, 15\}$ and $|H| = 3$.
(*b*) $H,\ 1 + H = \{1, 6, 11, 16\},\ 2 + H = \{2, 7, 12, 17\},\ 3 + H = \{3, 8, 13, 18\},\ 4 + H = \{4, 9, 14, 19\}$.

12.57. (*a*) See Fig. 12-13
(*b*) $5^{-1} = 11,\ 7^{-1} = 13,\ 17^{-1} = 17$.
(*c*) (i) $gp(5) = G$, $|5| = 6$; (ii) $gp(13) = \{1, 7, 13\}$, $|13| = 3$.
(*d*) Yes, since $G = gp(5)$.

×	1	5	7	11	13	17
1	1	5	7	11	13	17
5	5	7	17	1	11	13
7	7	17	13	5	1	11
11	11	1	5	13	17	7
13	13	11	1	17	7	5
17	17	13	11	7	5	1

Fig. 12-13

12.58. (*a*) $|1| = 1$, $|5| = 2$, $|7| = 2$, $|11| = 2$; (*b*) No; (*c*) $G, \{1\}, \{1, 7\}, \{1, 5\}, \{1, 11\}$.

12.59. (*a*)

$$\alpha\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}, \qquad \beta\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

$$\alpha^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \qquad \alpha^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}.$$

(*b*) $|\alpha| = 4$, $|\beta| = 3$, $|\alpha\beta = 4$.

12.66. $f(1) = 0$; $f(i) = 1$; $f(-1) = 2$; $f(-i) = 3$.

12.74. (*a*) 1, 5, 7, 11; (*b*) 4, 10; (*c*) $\{2, 10\}$.

12.75. (*a*) $-2 = 28,\ -7 = 23,\ -11 = 19$.
(*b*) $7^{-1} = 13,\ 11^{-1} = 11,\ 26^{-1}$ does not exist since 26 is not a unit.

12.77. Show $-a = a$ using $a + a = (a + a)^2$. Then show $ab = -ba$ by $a + b = (a + b)^2$.

12.78. (*b*) -1 is the 0-element, and 0 is the 1-element.

12.96. Let $f: D \to \mathbf{C}$ map $\begin{bmatrix} a & -b \\ b & a \end{bmatrix}$ into $a + bi$. Show f is an isomorphism.

12.98. *Hint*: Use Problem 12.97.

12.100. (*a*) $-2,\ (3 \pm \sqrt{29})/2$; (*b*) $3,\ (-5 \pm \sqrt{17})/2$.

12.101. (*a*) $-\frac{1}{2},\ 1 \pm 2\sqrt{2}$; (*b*) $\frac{3}{2},\ (-1 \pm \sqrt{13})/2$

12.102. $2 \pm 3i$; $(1 \pm \sqrt{5})/2$.

12.103. $1 \pm i$; $(-1 \pm \sqrt{21})/2$.

© The McGraw–Hill Companies, 2004

Chapter 13

Languages, Grammars, Machines

13.1 INTRODUCTION

One may view a digital computer as a "machine" M with the following properties. At each step in time, M is in a certain "internal state", M reads some "input", M prints some "output" which depends only on its internal state and the input, and then, possibly, M changes its internal state. There are various ways to formalize the notion of a machine M, and there exists a hierarchy of such machines.

One may also define a "computable" function in terms of a special kind of a machine M (Turing machine) which yields a nonnegative integer output $M(n)$ for any given nonnegative integer input n. Since most data may be coded by such integers, the machine M can handle most kinds of data.

This chapter is devoted to these and related topics.

13.2 ALPHABET, WORDS, FREE SEMIGROUP

Consider a nonempty set A of symbols. A *word* or *string* w on the set A is a finite sequence of its elements. For example, the sequences

$$u = ababb \qquad \text{and} \qquad v = accbaaa$$

are words on $A = \{a, b, c\}$. When discussing words on A, we frequently call A the *alphabet*, and its elements are called *letters*. We will also abbreviate our notation and write a^2 for aa, a^3 for aaa, and so on. Thus, for the above words, $u = abab^2$ and $v = ac^2ba^3$.

The empty sequence of letters, denoted by λ (Greek letter lambda) or ε (Greek letter epsilon), or 1, is also considered to be a word on A, called the *empty word*. The set of all words on A is denoted by A^*.

The *length* of a word u, written $|u|$ or $l(u)$, is the number of elements in its sequence of letters. For the above words u and v, we have $l(u) = 5$ and $\lambda(v) = 7$. Also, $l(\lambda) = 0$, where λ is the empty word.

Remark: Unless otherwise stated, the alphabet A will be finite, the symbols u, v, w will be reserved for words on A, and the elements of A will come from the letters a, b, c.

Concatenation

Consider two words u and v on alphabet A. The *concatenation* of u and v, written uv, is the word obtained by writing down the letters of u followed by the letters of v. For example, for the above words u and v, we have

$$uv = ababbaccbaaa = abab^2ac^2ba^3$$

As with letters, we define $u^2 = uu$, $u^3 = uuu$, and, in general, $u^{n+1} = uu^n$, where u is a word.

Clearly, for any words u, v, w, the words $(uv)w$ and $u(vw)$ are identical, they simply consist of the letters of u, v, w written down one after the other. Also, adjoining the empty word before or after a word u does not change the word u. In other words:

Theorem 13.1: The concatenation operation for words on an alphabet A is associative. The empty word λ is an identity element for the operation.

(Generally speaking, the operation is not commutative, e.g., $uv \neq vu$ for the above words u and v.)

Subwords, Initial Segments

Consider any word $u = a_1a_2 \cdots a_n$ on an alphabet A. Any sequence $w = a_ja_{j+1} \cdots a_k$ is called a *subword* of u. In particular, the subword $w = a_1a_2 \cdots a_k$, beginning with the first letter of u, is called

an *initial segment* of u. In other words, w is a subword of u if $u = v_1 w v_2$, and w is an initial segment of u if $u = wv$. Observe that λ and u are both subwords of u since $u = \lambda u$.

Consider the word $u = abca$. The subwords and initial segments of u follow:

(1) Subwords: λ, a, b, c, ab, bc, ca, abc, bca, $abca$.
(2) Initial segments: λ, a, ab, abc, $abca$.

Observe that the subword $w = a$ appears in two places in u. The word ac is not a subword of u even though all its letters belong to u.

Free Semigroup, Free Monoid

Let F denote the set of all nonempty words from an alphabet A with the operation of concatenation. As noted above, the operation is associative. Thus F is a semigroup; it is called the *free semigroup over A* or the *free semigroup generated by A*. One can easily show that F satisfies the right and left cancelation laws. However, F is not commutative when A has more than one element. We will write F_A for the free semigroup over A when we want to specify the set A.

Now let $M = A^*$ be the set of all words from A including the empty word λ. Since λ is an identity element for the operation of concatenation, M is a monoid, called the *free monoid* over A.

13.3 LANGUAGES

A *language L over* an alphabet A is a collection of words on A. Recall that A^* denotes the set of all words on A. Thus a language L is simply a subset of A^*.

EXAMPLE 13.1 Let $A = \{a, b\}$. The following are languages over A.

(*a*) $L_1 = \{a, ab, ab^2, \ldots\}$.
(*b*) $L_2 = \{a^m b^n : m > 0, n > 0\}$.
(*c*) $L_3 = \{a^m b^m : m > 0\}$.
(*d*) $L_4 = \{b^m a b^n : m \geq 0, n \geq 0\}$.

One may verbally describe these languages as follows.

(*a*) L_1 consists of all words beginning with an a and followed by zero or more b's.
(*b*) L_2 consists of all words beginning with one or more a's followed by one or more b's.
(*c*) L_3 consists of all words beginning with one or more a's and followed by the same number of b's.
(*d*) L_4 consists of all words with exactly one a.

Operations on Languages

Suppose L and M are languages over an alphabet A. Then the "concatenation" of L and M, denoted by LM, is the language defined as follows:

$$LM = \{uv : u \in L, v \in M\}$$

That is LM denotes the set of all words which come from the concatenation of a word from L with a word from M. For example, suppose

$$L_1 = \{a, b^2\} \qquad L_2 = \{a^2, ab, b^3\}, \qquad L_3 = \{a^2, a^4, a^6, \ldots\}$$

Then

$$L_1 L_2 = \{a^3, a^2 b, ab^3, b^2 a^2, b^2 ab, b^5\}$$
$$L_1 L_3 = \{a^3, a^5, a^7, \ldots, b^2 a^2, b^2 a^4, b^2 a^6, \ldots\}$$
$$L_1 L_1 = \{a^2, ab^2, b^2 a, b^4\}$$

Clearly, the concatenation of languages is associative since the concatenation of words is associative.

Powers of a language L are defined as follows:

$$L^0 = \{\lambda\}, \qquad L^1 = L, \qquad L^2 = LL, \qquad L^{m+1} = L^m L \text{ for } m > 1.$$

The unary operation L^* (read "L star") of a language L, called the *Kleene closure* of L because Kleene proved Theorem 13.2, is defined as the infinite union

$$L^* = L^0 \cup L^1 \cup L^2 \cup \cdots = \bigcup_{k=0}^{\infty} L^k$$

The definition of L^* agrees with the notation A^* which consists of all words over A. Some texts define L^+ to be the union of $L^1, L^2, \ldots$, that is, L^+ is the same as L^* but without the empty word λ.

13.4 REGULAR EXPRESSIONS, REGULAR LANGUAGES

Let A be a (nonempty) alphabet. This section defines a regular expression r over A and a language $L(r)$ over A associated with the regular expression r. The expression r and its corresponding language $L(r)$ are defined inductively as follows.

Definition: Each of the following is a regular expression over an alphabet A.

(1) The symbol "λ" (empty word) and the pair "( )" (empty expression) are regular expressions.
(2) Each letter a in A is a regular expression.
(3) If r is a regular expression, then (r^*) is a regular expression.
(4) If r_1 and r_2 are regular expressions, then $(r_1 \vee r_2)$ is a regular expression.
(5) If r_1 and r_2 are regular expressions, then $(r_1 r_2)$ is a regular expression.

All regular expressions are formed in this way.

Observe that a regular expression r is a special kind of a word (string) which uses the letters of A and the five symbols

$$(\qquad)\qquad *\qquad \vee\qquad \lambda$$

We emphasize that no other symbols are used for regular expressions.

Definition: The language $L(r)$ over A defined by a regular expression r over A is as follows:

(1) $L(\lambda) = \{\lambda\}$ and $L((\quad)) = \varnothing$, the empty set.
(2) $L(a) = \{a\}$, where a is a letter in A.
(3) $L(r^*) = (L(r))^*$ [the Kleene closure of $L(r)$].
(4) $L(r_1 \vee r_2) = L(r_1) \cup L(r_2)$ (the union of the languages).
(5) $L(r_1 r_2) = L(r_1)L(r_2)$ (the concatenation of the languages).

Remark: Parentheses will be omitted from regular expressions when possible. Since the concatenation of languages and the union of languages are associative, many of the parentheses may be omitted. Also, by adopting the convention that "$*$" takes precedence over concatenation, and concatenation takes precedence over "$\vee$", other parentheses may be omitted.

Definition: Let L be a language over A. Then L is called a *regular language* over A if there exists a regular expression r over A such that $L = L(r)$.

EXAMPLE 13.2 Let $A = \{a, b\}$. Each of the following is an expression r and its corresponding language $L(r)$:

(*a*) Let $r = a^*$. Then $L(r)$ consists of all powers of a, i.e., all words in a (including the empty word λ).

(*b*) Let $r = aa^*$. Then $L(r)$ consists of all positive powers of a, i.e., all words in a excluding the empty word.

(*c*) Let $r = a \vee b^*$. Then $L(r)$ consists of a or any word in b, that is,

$$L(r) = \{a, \lambda, b, b^2, \ldots\}$$

(*d*) Let $r = (a \vee b)^*$. Note $L(a \vee b) = \{a\} \cup \{b\} = A$; hence $L(r) = A^*$, all words over A.

(*e*) Let $r = (a \vee b)^*bb$. Then $L(r)$ consists of the concatenation of any word in A with bb, that is, all words ending in b^2.

(*f*) Let $r = a \wedge b^*$. $L(r)$ does not exist since r is not a regular expression. (Note $\wedge$ is not one of the symbols used for regular expressions.)

EXAMPLE 13.3 Consider the following languages over $A = \{a, b\}$:

(*a*) $L_1 = \{a^m b^n : m > 0, n > 0\}$

(*b*) $L_2 = \{b^m a b^n : m > 0, n > 0\}$

(*c*) $L_3 = \{a^m b^m : m > 0\}$.

Find a regular expression r over $A = \{a, b\}$ such that $L_i = L(r)$ for $i = 1, 2, 3$.

(*a*) L_1 consists of those words beginning with one or more a's followed by one or more b's. Hence we can set $r = aa^*bb^*$. Note that r is not unique; for example, $r = a^*abb^*$ is another solution.

(*b*) L_2 consists of all words which begin with one or more b's followed by a single a which is then followed by one or more b's, that is, all words with exactly one a which is neither the first nor the last letter. Hence $r = bb^*abb^*$ is a solution.

(*c*) L_3 consist of all words beginning with one or more a's followed by the same number of b's. There exists no regular expression r such that $L_3 = L(r)$; that is, L_3 is not a regular language. The proof of this fact appears in Example 13.7.

13.5 FINITE STATE AUTOMATA

A *finite state automaton* (FSA) or, simply, an *automaton* M consists of five parts:

(1) A finite set (alphabet) A of inputs.
(2) A finite set S of (internal) states.
(3) A subset Y of S (whose elements are called accepting or "yes" states).
(4) An initial state s_0 in S.
(5) A next-state function F from $S \times A$ into S.

Such an automaton M is denoted by $M = (A, S, Y, s_0, F)$ when we want to indicate its five parts. (The plural of automaton is automata.)

Some texts define the next-state function $F: S \times A \to S$ in (5) by means of a collection of functions $f_a: S \to S$, one for each $a \in A$; that is, each input a may be viewed as causing a change in the state of the automaton M. Setting $F(s, a) = f_a(s)$ shows that both definitions are equivalent.

EXAMPLE 13.4 The following defines an automaton M with two input symbols and three states:

(1) $A = \{a, b\}$, input symbols.
(2) $S = \{s_0, s_1, s_2\}$, internal states.
(3) $Y = \{s_0, s_1\}$, "yes" states.
(4) s_0, initial state.
(5) Next-state function $F: S \times A \to S$ defined by

$$F(s_0, a) = s_0, \quad F(s_1, a) = s_0, \quad F(s_2, a) = s_2$$
$$F(s_0, b) = s_1, \quad F(s_1, b) = s_2, \quad F(s_2, b) = s_2$$

The next-state function F is frequently given by means of a table as in Fig. 13-1.

F	a	b
s_0	s_0	s_1
s_1	s_0	s_2
s_2	s_2	s_2

Fig. 13-1

State Diagram of an Automaton M

An automaton M is usually defined by means of its state diagram $D = D(M)$ rather than by listing its five parts. The state diagram $D = D(M)$ is a labeled directed graph as follows.

(1) The vertices of $D(M)$ are the states in S and an accepting state is denoted by means of a double circle.
(2) There is an arrow (directed edge) in $D(M)$ from state s_j to state s_k labeled by an input a if $F(s_j, a) = s_k$ or, equivalently, if $f_a(s_j) = s_k$.
(3) The initial state s_0 is indicated by means of a special arrow which terminates at s_0 but has no initial vertex.

For each vertex s_j and each letter a in the alphabet A, there will be an arrow leaving s_j which is labeled by a; hence the outdegree of each vertex is equal to number of elements in A. For notational convenience, we label a single arrow by all the inputs which cause the same change of state rather than having an arrow for each such input.

The state diagram $D = D(M)$ of the automaton M in Example 13.1 appears in Fig. 13-2. Note that both a and b label the arrow from s_2 to s_2 since $F(s_2, a) = s_2$ and $F(s_2, b) = s_2$. Note also that the outdegree of each vertex is 2.

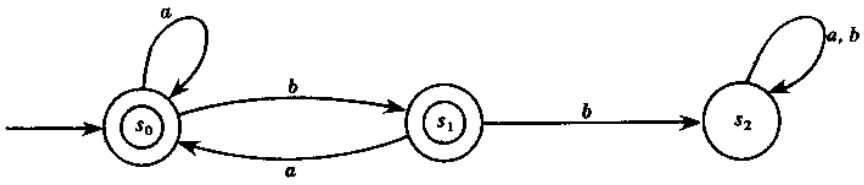


Fig. 13-2

Language $L(M)$ Determined by an Automaton M

Each automaton M with input alphabet A defines a language over A, denoted by $L(M)$, as follows.

Let $w = a_1 a_2 \cdots a_m$ be a word on A. Then w determines a sequence of states

$$s_0 \to s_1 \to s_2 \to \cdots \to s_m$$

where s_0 is the initial state and $F(s_{i-1},\ a_i) = s_i$ for $i \geq 1$. In other words, W determines the path

$$P = (s_0,\ a_1,\ s_1,\ a_2,\ s_2, \ldots, a_m,\ s_m)$$

in the state diagram graph $D(M)$.

We say that M *recognizes* the word w if the final state s_m is an accepting state in Y. The language $L(M)$ of M is the collection of all words from A which are accepted by M.

EXAMPLE 13.5

(*a*) Determine whether or not the automaton M in Fig 13-2 accepts the word w where:

(1) $w = ababba$; (2) $w = baab$; (3) $w = \lambda$.

(1) Use Fig. 13-2 and the word $w = ababba$ to obtain the path

$$P = s_0 \xrightarrow{a} s_0 \xrightarrow{b} s_1 \xrightarrow{a} s_0 \xrightarrow{b} s_1 \xrightarrow{b} s_2 \xrightarrow{a} s_2$$

The final state s_2 is not in Y; hence w is not accepted by M.

(2) The word $w = baab$ determines the path

$$P = s_0 \xrightarrow{b} s_1 \xrightarrow{a} s_0 \xrightarrow{a} s_0 \xrightarrow{b} s_1$$

The final state s_1 is in Y; hence w is accepted by M.

(3) Here the final state is the initial state s_0 since w is the empty word. Since s_0 is in Y, λ is accepted by M.

(*b*) Describe the language $L(M)$ of the automaton M in Fig. 13-2.

$L(M)$ will consist of all words w from A which do not have two successive b's. This comes from the following facts:

(1) We can enter the state s_2 only after two successive b's.

(2) We can never leave s_2.

(3) The state s_2 is the only rejecting (nonaccepting) state.

The fundamental relationship between regular languages and automata is contained in the following theorem (whose proof lies beyond the scope of this text).

Theorem 13.2 (Kleene): A language L over an alphabet A is regular if and only if there is a finite state automaton M such that $L = L(M)$.

The star operation L^* on a language L is sometimes called the Kleene closure of L since Kleene first proved the above basic result.

EXAMPLE 13.6 Let $A = \{a, b\}$. Construct an automaton M which will accept precisely those words from A which end in two b's.

Since b^2 is accepted, but not λ or b, we need three states, s_0, the initial state, and s_1 and s_2 with an arrow labeled b going from s_0 to s_1 and one from s_1 to s_2. Also, s_2 is an accepting state, but not s_0 and s_1. This gives the graph in Fig. 13-3(*a*). On the other hand, if there is an a, then we want to go back to s_0, and if we are in s_2 and there is a b, then we want to stay in s_2. These additional conditions give the required automaton M which is shown in Fig. 13-3(*b*).

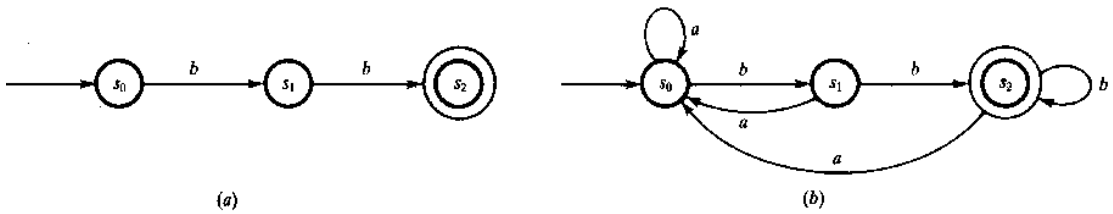


Fig. 13-3

Pumping Lemma

Suppose an automaton M over A has k states, and suppose $w = a_1 a_2 \cdots a_n$ is a word over A accepted by M such that $|w| = n > k$, the number of states. Let

$$P = (s_0, s_1, \cdots, s_n)$$

be the corresponding sequence of states determined by the word w. Since $n > k$, two of the states in P must be equal, say $s_i = s_j$ where $i < j$. Let

$$x = a_1 a_2 \cdots a_i, \qquad y = a_{i+1} \cdots a_j, \qquad z = a_{j+1} \cdots a_n$$

As shown in Fig. 13-4, xy ends in $s_i = s_j$; hence xy^m also ends in s_i. Thus, for every m, $w_m = xy^m z$ ends in s_n, which is an accepting state.

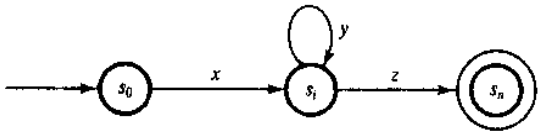


Fig. 13-4

The above discussion proves the following important result.

Theorem 13.3 (Pumping Lemma): Suppose M is an automaton over A such that:

(i) M has k states.

(ii) M accepts a word w from A where $|w| > k$.

Then $w = xyz$ where, for every positive m, $w_m = xy^m z$ is accepted by M.

The next example gives an application of the Pumping Lemma.

EXAMPLE 13.7 Show that the language $L = \{a^m b^m : m \text{ positive}\}$ is not regular.

Suppose L is regular. Then, by Theorem 13.2, there exists a finite state automaton M which accepts L. Suppose M has k states. Let $w = a^k b^k$. Then $|w| > k$. By the Pumping Lemma (Theorem 13.3), $w = xyz$ where y is not empty and $w_2 = xy^2 z$ is also accepted by M. If y consists of only a's or only b's, then w_2 will not have the same number of a's as b's. If y contains both a's and b's, then w_2 will have a's following b's. In either case w_2 does not belong to L, which is a contradiction. Thus L is not regular.

13.6 GRAMMARS

Figure 13-5 shows the grammatical construction of a specific sentence. Observe that there are:

(1) various variables, e.g., ⟨sentence⟩, ⟨noun phrase⟩, ...;

(2) various terminal words, e.g., "The", "boy", ...;

(3) a beginning variable ⟨sentence⟩; and

(4) various substitutions or productions, e.g.

$$\langle \text{sentence} \rangle \rightarrow \langle \text{noun phrase} \rangle \ \langle \text{verb phrase} \rangle$$
$$\langle \text{object phrase} \rangle \rightarrow \langle \text{article} \rangle \ \langle \text{noun} \rangle$$
$$\langle \text{noun} \rangle \rightarrow \text{apple}$$

The final sentence only contains terminals, although both variables and terminals appear in its construction by the productions. This intuitive description is given in order to motivate the following definition of a grammar and the language it generates.

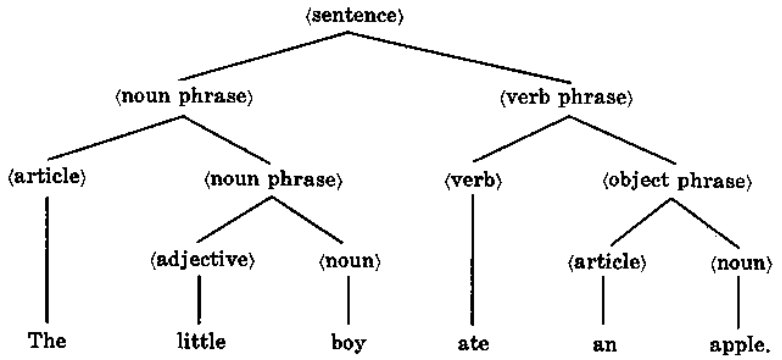


Fig. 13-5

A *phrase structure grammar* or, simply, a *grammar* G consists of four parts:

(1) A finite set (*vocabulary*) V.
(2) A subset T of V whose elements are called *terminals*; the elements of $N = V \setminus T$ are called *nonterminals* or *variables*.
(3) A nonterminal symbol S called the *start* symbol.
(4) A finite set P of productions. A production is an ordered pair (α, β) usually written $\alpha \to \beta$, where α and β are words in V. Each production in P must contain at least one nonterminal on its left side.

Such a grammar G is denoted by $G = G(V, T, S, P)$ when we want to indicate its four parts.

The following notation, unless otherwise stated or implied, will be used for our grammars. Terminals will be denoted by italic lower case Latin letters, $a, b, c, \ldots$, and nonterminals will be denoted by italic capital Latin letters, $A, B, C, \ldots$ with S as the start symbol. Also, Greek letters, $\alpha, \beta, \ldots$ will denote words in V, that is, words in terminals and nonterminals. Furthermore, we will write

$$\alpha \to (\beta_1, \beta_2, \ldots, \beta_k) \qquad \text{instead of} \qquad \alpha \to \beta_1,\ \alpha \to \beta_2, \ldots,\ \alpha \to \beta_k,$$

Remark: Frequently, we will define a grammar G by only giving its productions, assuming implicitly that S is the start symbol and that the terminals and nonterminals of G are only those appearing in the productions.

EXAMPLE 13.8 The following defines a grammar G:

$$V = \{A, B, S, a, b\}, \qquad T = \{a, b\}, \qquad P = \{S \xrightarrow{1} AB, A \xrightarrow{2} Aa, B \xrightarrow{3} Bb, A \xrightarrow{4} a, B \xrightarrow{5} b\}$$

with S as the start symbol. The productions may be abbreviated as follows:

$$S \to AB, \qquad A \to (Aa, a), \qquad B \to (Bb, b)$$

Language $L(G)$ of a Grammar G

Suppose w and w' are words over the vocabulary set V of a grammar G. We write

$$w \Rightarrow w'$$

if w' can be obtained from w by using one of the productions; that is, if there exists words u and v such that $w = u\alpha v$ and $w' = u\beta v$ and there is a production $\alpha \to \beta$. We write

$$w \Rightarrow\Rightarrow w' \qquad \text{or} \qquad w \overset{*}{\Rightarrow} w'$$

if w' can be obtained from w using a finite number of productions.

Now let G be a grammar with terminal set T. The language of G, denoted by $L(G)$, consists of all words in T that can be obtained from the start symbol S by the above process; that is,

$$L(G) = \{w \in T^*: S \Rightarrow\Rightarrow w\}$$

EXAMPLE 13.9 Consider the grammar G in Example 13.8. Observe that $w = a^2b^4$ can be obtained from the start symbol S as follows:

$$S \Rightarrow AB \Rightarrow AaB \Rightarrow aaB \Rightarrow aaBb \Rightarrow aaBbb \Rightarrow aaBbbb \Rightarrow aabbbb = a^2b^4$$

Here we used the productions 1, 2, 4, 3, 3, 3, 5, respectively. Thus we can write $S \Rightarrow\Rightarrow a^2b^4$. Hence $w = a^2b^4$ belongs to $L(G)$. More generally, the production sequence 1, 2 (r times), 4, 3 (s times), 5 will produce the word $w = a^rab^sb$ where r and s are nonnegative integers. On the other hand, no sequence of productions can produce an a after a b. Accordingly,

$$L(G) = \{a^mb^n: m \text{ and } n \text{ positive integers}\}$$

That is, the language $L(G)$ of the grammar G consists of all words which begin with one or more a's followed by one or more b's.

EXAMPLE 13.10 Find the language $L(G)$ over $\{a, b, c\}$ generated by the grammar G with productions

$$S \to aSb, \qquad aS \to Aa, \qquad Aab \to c$$

First we must apply the first production one or more times to obtain the word $w = a^nSb^n$ where $n > 0$. To eliminate S, we must apply the second production to obtain the word $w' = a^mAabb^m$ where $m = n - 1 \geq 0$. Now we can only apply the third production to finally obtain the word $w^n = a^mcb^m$ where $m \geq 0$. Accordingly,

$$L(G) = \{a^mcb^m: m \text{ nonnegative}\}$$

That is, $L(G)$ consists of all words with the same nonnegative number of a's and b's separated by a c.

Types of Grammars

Grammars are classified according to the kinds of production which are allowed. The following grammar classification is due to Noam Chomsky.

A Type 0 grammar has no restrictions on its productions. Types 1, 2, and 3 are defined as follows:

(1) A grammar G is said to be of Type 1 if every production is of the form $\alpha \to \beta$ where $|\alpha| \leq |\beta|$ or of the form $\alpha \to \lambda$.

(2) A grammar G is said to be of Type 2 if every production is of the form $A \to \beta$, i.e., where the left side is a nonterminal.

(3) A grammar G is said to be of Type 3 if every production is of the form $A \to a$ or $A \to aB$, i.e., where the left side is a single nonterminal and the right side is a single terminal or a terminal followed by a nonterminal, or of the form $S \to \lambda$.

Observe that the grammars form a hierarchy; that is, every Type 3 grammar is a Type 2 grammar, every Type 2 grammar is a Type 1 grammar, and every Type 1 grammar is a Type 0 grammar.

Grammars are also classified in terms of context-sensitive, contex-free, and regular as follows.

(a) A grammar G is said to be *context-sensitive* if the productions are of the form

$$\alpha A\alpha' \to \alpha\beta\alpha'$$

The name "context-sensitive" comes from the fact that we can replace the variable A by β in a word only when A lies between α and α'.

(*b*) A grammar G is said to be *context-free* if the productions are of the form

$$A \to \beta$$

The name "context-free" comes from the fact that we can now replace the variable A by β regardless of where A appears.

(*c*) A grammar G is said to be *regular* if the productions are of the form

$$A \to a, \qquad A \to aB, \qquad S \to \lambda$$

Observe that a contex-free grammar is the same as a Type 2 grammar, and a regular grammar is the same as a Type 3 grammar.

A fundamental relationship between regular grammars and finite automata follows.

Theorem 13.4: A language L can be generated by a Type 3 (regular) grammar G, if and only if there exists a finite automaton M which accepts L.

Thus a language L is regular iff $L = L(r)$ where r is a regular expression iff $L = L(M)$ where M is a finite automaton iff $L = L(G)$ where G is a regular grammar. (Recall that iff is an abbreviation for "if and only if".)

EXAMPLE 13.11 Consider the language $L = \{a^n b^n;\ n > 0\}$.

(*a*) Find a contex-free grammar G which generates L.

Clearly the grammar G with the following productions will generate G:

$$S \to ab, \qquad S \to aSb$$

Note that G is a context-free language since each left side is a nonterminal.

(*b*) Find a regular grammar G which generates L.

By Example 13.7, L is not a regular language. Thus L cannot be generated by a regular grammar.

Derivation Trees of Context-free Grammars

Consider a contex-free (Type 2) grammar G. Any derivation of a word w in $L(G)$ can be represented graphically by means of an ordered, rooted tree T, called a *derivation* or *parse* tree. For example, let G be the contex-free grammar with the following productions:

$$S \to aAB, \qquad A \to Bba, \qquad B \to bB, \qquad B \to c$$

The word $w = acbabc$ can be derived from S as follows:

$$S \Rightarrow aAB \to a(Bba)B \Rightarrow acbaB \Rightarrow acba(bB) \Rightarrow acbabc$$

One can draw a *derivation tree* T of the word w as indicated by Fig. 13-6. Specifically, we begin with S as the root and then add branches to the tree according to the production used in the derivation of w. This yields the completed tree T which is shown in Fig. 13-6(*e*). The sequence of leaves from left to right in T is the derived word w. Also, any nonleaf in T is a variable, say A, and the immediate successors (children) of A form a word α where $A \to \alpha$ is the production of G used in the derivation of w.

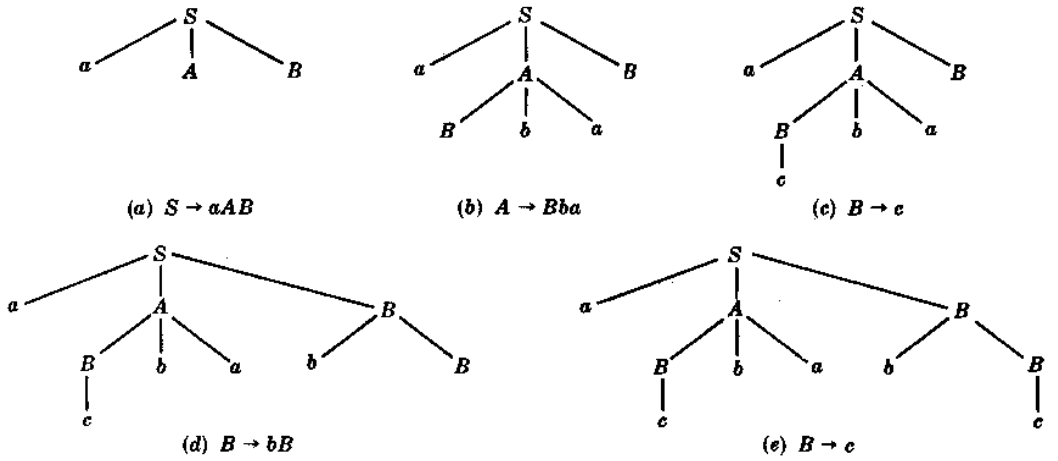


Fig. 13-6

Backus-Naur Form

There is another notation, called the Backus-Naur form, which is sometimes used for describing the productions of a contex-free (Type 2) grammar. Specifically:

(i) $::=$ is used instead of $\rightarrow$.

(ii) Every nonterminal is enclosed in brackets $\langle\ \rangle$.

(iii) All productions with the same nonterminal left-hand side are combined into one statement with all the right-hand sides listed on the right of $::=$, separated by vertical bars.

For instance, the productions $A \rightarrow aB$, $A \rightarrow b$, $A \rightarrow BC$ are combined into the one statement:

$$\langle A\rangle\ ::= a\langle B\rangle | b | \langle B\rangle\langle C\rangle$$

Machines and Grammars

Theorem 13.4 tells us that the regular languages correspond to the finite state automata (FSA). There are also machines, more powerful than the FSA, which correspond to the other grammars.

(*a*) ***Pushdown Automata***: A pushdown automaton P is similar to a FSA except that P has an auxiliary stack which provides an unlimited amount of memory for P. A language L is recognized by a pushdown automaton P if and only if L is context-free.

(*b*) ***Linear Bounded Automata***: A linear bounded automaton B is more powerful than a pushdown automaton. Such an automaton B uses a tape which is linearly bounded by the length of the input word w. A language L is recognized by a linear bounded automaton B if and only if L is context-sensitive.

(*c*) ***Turing Machine***: A Turing machine M, named after the British mathematician Alan Turing, uses an infinite tape; it is able to recognize every language L that can be generated by any phase-structure grammar G. In fact, a Turing machine M is one of a number of equivalent ways to define the notion of a "computable" function.

The discussion of the pushdown automata and the linear bounded automata lies beyond the scope of this text. We will discuss Turing machines in Section 13.8.

13.7 FINITE STATE MACHINES

A finite state machine (FSM) is similar to a finite state automaton (FSA) except that the finite state machine "prints" an output using an output alphabet distinct from the input alphabet. The formal definition follows.

A *finite state machine* (or *complete sequential machine*) M consists of six parts:

(1) A finite set A of input symbols.
(2) A finite set S of "internal" states.
(3) A finite set Z of output symbols.
(4) An initial state s_0 in S.
(5) A next-state function f from $S \times A$ into S.
(6) An output function g from $S \times A$ into Z.

Such a machine M is denoted by $M = M(A, S, Z, s_0, f, g)$ when we want to indicate its six parts.

EXAMPLE 13.12 The following defines a finite state machine M with two input symbols, three internal states, and three output symbols:

(1) $A = \{a, b\}$.
(2) $S = \{s_0, s_1, s_2\}$.
(3) $Z = \{x, y, z\}$.
(4) Initial state s_0.
(5) Next-state function $f: S \times A \to S$ defined by

$$f(s_0, a) = s_1, \quad f(s_1, a) = s_2, \quad f(s_2, a) = s_0$$
$$f(s_0, b) = s_2, \quad f(s_1, b) = s_1, \quad f(s_2, b) = s_1$$

(6) Output function $g: S \times A \to Z$ defined by

$$g(s_0, a) = x, \quad g(s_1, a) = x, \quad g(s_2, a) = z$$
$$g(s_0, b) = y, \quad g(s_1, b) = z, \quad f(s_2, b) = y$$

State Table and State Diagram of a Finite State Machine

There are two ways of representing a finite state machine M in compact form. One way is by a table called the *state table* of the machine M, and the other way is by a labeled directed graph called the *state diagram* of the machine M.

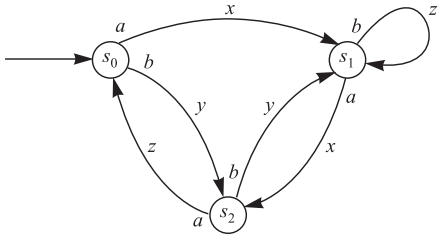
The state table combines the next-state function f and the output function g into a single table which represent the function $F: S \times A \to S \times Z$ defined by

$$F(s_i, a_j) = (f(s_i, a_j), g(s_i, a_j))$$

For instance, the state table of the machine M in Example 13.12 is pictured in Fig. 13-7(a). The states are listed on the left of the table with the initial state first, and the input symbols are listed on the top of the table. The entry in the table is a pair (s_k, z_r) where $s_k = f(s_i, a_j)$ is the next state and $z_r = g(s_i, a_j)$ is the output symbol. One assumes that there are no output symbols other than those appearing in the table.

F	a	b
s_0	s_1, x	s_2, y
s_1	s_2, x	s_1, y
s_2	s_0, x	s_1, y

(a)



(b)

Fig. 13-7

The state diagram $D = D(M)$ of a finite state machine $M = M(A, S, Z, s_0, f, g)$ is a labeled directed graph. The vertices of D are the states of M. Moreover, if

$$F(s_i, a_j) = (s_k, z_r), \qquad \text{that is,} \qquad f(s_i, a_j) = s_k \qquad \text{and} \qquad g(s_i, a_j) = z_r$$

then there is an arc (arrow) from s_i to s_k which is labeled with the pair a_j, z_r. We usually put the input symbol a_j near the base of the arrow (near s_i) and the output symbol z_r near the center of the arrow. We also label the initial state s_0 by drawing an extra arrow into s_0. For instance, the state diagram of the machine M in Example 13.12 appears in Fig. 13-7(b).

Input and Output Tapes

The above discussion of a finite state machine M does not show the dynamic quality of M. Suppose M is given a string (word) of input symbols, say

$$u = a_1 a_2 \cdots a_m$$

We visualize these symbols on an "input tape"; the machine M "reads" these input symbols one by one and, simultaneously, changes through a sequence of states

$$v = s_0 s_1 s_2 \cdots s_m$$

where s_0 is the initial state, while printing a string (word) of output symbols

$$w = z_1 z_2 \cdots z_m$$

on an "output tape". Formally, the initial state s_0 and the input string u determine the strings v and w by

$$s_i = f(s_{i-1},\ a_i) \qquad \text{and} \qquad z_i = g(s_{i-1},\ a_i)$$

where $i = 1, 2, \ldots, m$.

EXAMPLE 13.13 Consider the machine M in Fig. 13-7, that is, Example 13.12. Suppose the input is the word

$$u = abaab$$

We calculate the sequence v of states and the output word w from the state diagram as follows. Beginning at the initial state s_0 we follow the arrows which are labeled by the input symbols as follows:

$$s_0 \xrightarrow{a,x} s_1 \xrightarrow{b,z} s_1 \xrightarrow{a,x} s_2 \xrightarrow{a,z} s_0 \xrightarrow{b,y} s_2$$

This yields the following sequence v of states and output word w:

$$v = s_0 s_1 s_1 s_2 s_0 s_2 \qquad \text{and} \qquad w = xzxzy$$

Binary Addition

This subsection describes a finite state machine M which can do binary addition. By adding 0's at the beginning of our numbers, we can assume that our numbers have the same number of digits. If the machine is given the input

$$\begin{array}{r} 1101011 \\ +\,0111011 \\ \hline \end{array}$$

then we want the output to be the binary sum

$$10100110$$

Specifically, the input is the string of pairs of digits to be added:

$$11, \quad 11, \quad 00, \quad 11, \quad 01, \quad 11, \quad 10, \quad b$$

where b denotes blank spaces, and the output should be the string

$$0, \quad 1, \quad 1, \quad 0, \quad 0, \quad 1, \quad 0, \quad 1$$

We also want the machine to enter a state called "stop" when the machine finishes the addition.

The input symbols are

$$A = \{00, 01, 10, 11, b\}$$

and the output symbols are

$$Z = \{0, 1, b\}$$

The machine that we "construct" will have three states:

$$S = \{\text{carry } (c), \text{ no carry } (n), \text{ stop } (s)\}$$

Here n is the initial state. The machine is shown in Fig. 13-8.

In order to show the limitations of our machines, we state the following theorem.

Theorem 13.5: There is no finite state machine M which can do binary multiplication.

If we limit the size of the numbers that we multiply, then such machines do exist. Computers are important examples of finite machines which multiply numbers, but the numbers are limited as to their size.

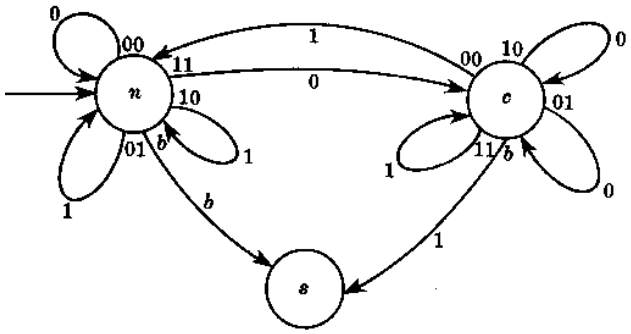


Fig. 13-8

13.8 GÖDEL NUMBERS

Recall (Section 11.5) that a positive integer $p > 1$ is called a prime number if its only positive divisors are 1 and p. We let $p_1, p_2, \ldots$ denote the successive prime numbers. Thus

$$p_1 = 2, \qquad p_2 = 3, \qquad p_3 = 5, \qquad p_4 = 7, \qquad p_5 = 11, \qquad \ldots$$

(By Theorem 11.11, there exists an infinite number of primes.) The Fundamental Theorem of Arithmetic (Theorem 11.19) states that any positive integer $n > 1$ can be written uniquely (except for order) as a product of prime numbers. The German logician Kurt Gödel used this result to code finite sequences of numbers and also to code words over a finite or countable alphabet. Each sequence or word is assigned a positive integer called its *Gödel number* as follows.

The *Gödel number* of the sequence $s = (n_1, n_2, \ldots, n_k)$ of nonnegative integers is the positive integer $c(s)$ where n_i is the exponent of p_i in the prime decomposition of $c(s)$, that is,

$$c(s) = {p_1}^{n_1} {p_2}^{n_2} \ldots {p_k}^{n_k}$$

For example,

$$c = (3, 1, 2, 0, 2) \qquad \text{is coded by} \qquad c(s) = 2^3 \cdot 3 \cdot 5^2 \cdot 7^0 \cdot 11^2 = 72\,600$$

The Gödel number of a word w on an alphabet $\{a_0, a_1, a_2, a_3, \ldots, \}$ is the positive integer $c(w)$ where the subscript of the ith letter of w is the exponent of p_i in the prime decomposition of $c(w)$. For instance,

$$w = a_4a_1a_3a_2a_2 \qquad \text{is coded by} \qquad c(w) = 2^4 \cdot 3 \cdot 5^3 \cdot 7^2 \cdot 11^2 = 35\,574\,000$$

(Observe that both codes are essentially the same since we may view a word w as the sequence of the subscripts of its letters.)

The above coding is essentially the proof of the main result of this section:

Theorem 13.6: Suppose an alphabet A is countable. Then any language L over A is also countable.

Proof: The Gödel coding is a one-to-one mapping $c: L \to \mathbf{N}$. Thus L is countable.

13.9 TURING MACHINES

There are a number of equivalent ways to formally define a "computable" function. We do it by means of a Turing machine M. This section formally defines a Turing machine M, and the next section defines a computable function.

Our definition of a Turing machine uses an infinite two-way tape, quintuples, and three halt states. Other definitions use a one-way infinite tape and/or quadruples, and one halt state. However, all the definitions are equivalent.

Basic Definitions

A Turing machine M involves three disjoint nonempty sets:

(1) A finite *tape* set

$$A = \{a_1, a_2, \cdots, a_m\} \cup \{B\}$$

Here $B = a_0$ is the "blank" symbol.

(2) A finite *state* set

$$S = \{s_1, s_2, \cdots, s_n\} \cup \{s_0\} \cup \{s_H, s_Y, s_N\}$$

Here s_0 is the *initial state*. Furthermore, s_H (HALT) is the halting state, s_Y (YES) is the accepting state, and S_N (NO) is the nonaccepting state.

(3) A *direction* set

$$d = \{L, R, N\}$$

Here L denotes "left", R denotes "right", and N denotes "no movement" or "stay".

Definition 1.1: An *expression* is a finite (possibly empty) sequence of elements from $A \cup S \cup d$.

In other words, an expression is a word whose letters (symbols) come from the sets A, S, and d.

Definition 1.2: A *tape expression* is an expression using only elements from the tape set A.

The Turing machine M may be viewed as a read/write tape head which moves back and forth along an infinite tape. The tape is divided lengthwise into squares (cells), and each square may be blank or hold one tape symbol. At each step in time, the Turing machine M is in a certain internal state s_i scanning one of the tape symbols a_j on the tape. We assume that only a finite number of nonblank symbols appear on the tape.

Figure 13-9(a) is a picture of a Turing machine M in state s_2 scanning the second symbol where $a_1a_3Ba_1a_1$ is printed on the tape. (Note again that B is the blank symbol.) This picture may be represented by the expression $\alpha = a_1s_2a_3Ba_1a_1$ where we write the state s_2 of M before the tape symbol a_3 that M is scanning. Observe that α is an expression using only the tape alphabet A except for the state symbol

s_2 which is not at the end of the expression since it appears before the tape symbol a_3 that M is scanning. Figure 13-9 shows two other informal pictures and their corresponding picture expressions.

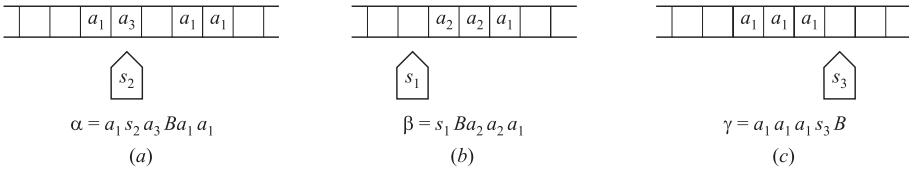


Fig. 13-9

We give formal definitions.

Definition 1.3: A *picture* α is an expression of the form

$$\alpha = Ps_i a_k Q$$

where P and Q are tape expressions (possibly empty).

Definition 1.4: Let $\alpha = Ps_i a_k Q$ be a picture. We say that the Turing machine M is *in state* s_i *scanning the letter* a_k and that the *expression on the tape* is the expression $Pa_k Q$, that is, α without its state symbol s_i.

As mentioned above, at each step in time the turing machine M is in a certain state s_i and is scanning a tape symbol a_k. The Turing machine M is able to do the following three things simultaneously:

(i) M erases the scanned symbol a_k and writes in its place a tape symbol a_ℓ (where we permit $a_\ell = a_k$).

(ii) M changes its internal states s_i to a state s_j (where we permit $s_j = s_i$).

(iii) M moves one square to the left, moves one square to the right, or does not move at all.

The above action by M may be described by a five-letter expression called a *quintuple* which we define below.

Definition 1.5: A *quintuple* q is a five-letter expression of the following form:

$$q = (s_i, a_k, a_\ell, s_j, \begin{Bmatrix} L \\ R \\ N \end{Bmatrix})$$

That is, the first letter of q is a state symbol, the second is a tape symbol, the third is a tape symbol, the fourth is a state symbol, and the last is a direction symbol L, R, or N.

Next we give a formal definition of a Turing machine.

Definition 1.6: A Turing machine M is a finite set of quintuples such that:

(i) No two quintuples begin with the same first two letters.

(ii) No quintuple begins with s_H, s_Y, or s_N.

Condition (i) in the definition guarantees that the machine M cannot do more than one thing at any given step, and condition (ii) guarantees that M halts in state s_H, s_Y, or s_N.

The following is an alternative equivalent definition.

Definition 1.6′: A Turing machine M is a partial function from

$$S\backslash\{s_H, s_Y, s_N\} \times A \qquad \text{into} \qquad A \times S \times d$$

The term partial function simply means that domain of M is a subset of $S\backslash\{s_H, s_Y, s_N\} \times A$.

The action of the Turing machine described above can now be formally defined.

Definition 1.7: Let α and β be pictures. We write

$$\alpha \to \beta$$

if one of the following holds where a, b, c are tape letters and P and Q are tape expressions (possibly empty):

(i) $\alpha = Ps_iaQ$, $\beta = Ps_jbQ$ and M contains the quintuple $q = s_iabs_jN$.

(ii) $\alpha = Ps_iacQ$, $\beta = Pbs_jcQ$ and M contains the quintuple $q = s_iabs_jR$.

(iii) $\alpha = Pcs_iaQ$, $\beta = Ps_jcbQ$ and M contains the quintuple $q = s_iabs_jL$.

(iv) $\alpha = Ps_ia$, $\beta = Pbs_jB$ and M contains the quintuple $q = s_iabs_jR$.

(v) $\alpha = s_iaQ$, $\beta = s_jBbQ$ and M contains the quintuple $q = s_iabs_jL$.

Observe that, in all five cases, M replaces a on the tape by b (where we permit $b = a$), and M changes its state from s_i to s_j (where we permit $s_j = s_i$). Furthermore:

(i) Here M does not move.

(ii) Here M moves to the right.

(iii) Here M moves to the left.

(iv) Here M moves to the right; however, since M is scanning the rightmost letter, it must add the blank symbol B on the right.

(v) Here M moves to the left; however, since M is scanning the leftmost letter, it must add the blank symbol B on the left.

Definition 1.8: A picture α is said to be *terminal* if there is no picture β such that $\alpha \to \beta$.

In particular, any picture α in one of the three halt states must be terminal since no quintuple begins with s_H, s_Y, or s_N.

Computing with a Turing Machine

The above is a static (one-step) description of a Turing machine M. Now we discuss its dynamics.

Definition 1.9: A *computation* of a turing machine M is a sequence of pictures $\alpha_0, \alpha_1, \ldots, \alpha_m$ such that $\alpha_{i-1} \to \alpha_i$, for $i = 1, \ldots, m$, and α_m is a terminal picture.

In other words, a computation is a sequence

$$\alpha_0 \to \alpha_1 \to \alpha_2 \to \cdots \to \alpha_m$$

which cannot be extended since α_m is terminal. We will let $term(\alpha)$ denote the final picture of a computation beginning with α. Thus $\text{term}(\alpha_0) = \alpha_m$ in the above computation.

Turing Machines with Input

The following definition applies.

Definition 1.10: An *input* for a Turing machine M is a tape expression W. The *initial picture* for an input W is $\alpha(W)$ where $\alpha(W) = s_0W$.

Observe that the initial picture $\alpha(W)$ of the input W is obtained by placing the initial state s_0 in front of the input tape expression W. In other words, the Turing machine M begins in its initial state s_0 and it is scanning the first letter of W.

Definition 1.11: Let M be a Turing machine M and let W be an input. We say *M halts on W* if there is a computation beginning with the initial picture $\alpha(W)$.

That is, given an input W, we can form the initial picture $\alpha(W) = s_0 W$ and apply M to obtain the sequence

$$\alpha(W) \to \alpha_1 \to \alpha_2 \to \cdots$$

Two things can happen:

(1) *M halts on W.* That is, the sequence ends with some terminal picture α_r.
(2) *M does not halt on W.* That is, the sequence never ends.

Grammars and Turing Machines

Turing machines may be used to recognize languages. Specifically, suppose M is a Turing machine with tape set A. Let L be the set of words W in A such that M halts in the accepting state s_Y when W is the input. We will then write $L = L(M)$, and we will say that M *recognizes* the language L. Thus an input W does not belong to $L(M)$ if M does not halt on W or if M halts on W but not in the accepting state s_Y.

The following theorem is the main result of this subsection; its proof lies beyond the scope of this text.

Theorem 13.7: A language L is recognizable by a Turing machine M if and only if L is a type 0 language.

Remark: The reason for three halt states is that s_Y and s_N are used for recognizing languages, whereas s_H is used for computations discussed in the next section.

EXAMPLE 13.14 Suppose a Turing machine M with tape set $A = \{a, b, c\}$ contains the following four quintuples:

$$q_1 = s_0 a a s_0 R, \qquad q_2 = s_0 b b s_0 R, \qquad q_3 = s_0 B B s_N R, \qquad q_4 = s_0 c c s_Y N.$$

(*a*) Suppose $W = W(a, b, c)$ is an input without any c's.

By the quintuples q_1 and q_2, M stays in state s_0 and moves to the right until it encounters a blank symbol B. Then M changes its state to the nonaccepting state s_N and halts.

(*b*) Suppose $W = W(a, b, c)$ is an input with at least one c symbol.

By the quintuple q_4, when M initially meets the first c in W it changes its state to the accepting state by s_Y and halts.

Thus M recognizes the language L of all words W in a, b, c with at least one letter c. That is, $L = L(M)$.

13.10 COMPUTABLE FUNCTIONS

Computable functions are defined on the set of nonnegative integers. Some texts use $\mathbf{N}$ to denote this set. We use $\mathbf{N}$ to denote the set of positive integers, so we will use the notation

$$\mathbf{N}_0 = \{0, 1, 2, 3, \ldots\}$$

Throughout this section, the terms number, integer, and nonnegative integer are used synonymously.

The preceding section described the way a Turing machine M manipulates and recognizes character data. Here we show how M manipulates numerical data. First, however, we need to be able to represent our numbers by our tape set A. We will write 1 for the tape symbol a_1 and 1^n for $111 \cdots 1$, where 1 occurs n times.

Definition 2.1: Each number n will be represented by the tape expression $\langle n\rangle$ where $\langle n\rangle = 1^{n+1}$. Thus

$$\langle 4\rangle = 11111 = 1^5, \qquad \langle 0\rangle = 1, \qquad \langle 2\rangle = 111 = 1^3.$$

Definition 2.2: Let E be an expression. Then $[E]$ will denote the number of times 1 occurs in E. Thus

$$[11Bs_2a_3111Ba_4] = 5, \qquad [a_4s_2Ba_2] = 0, \qquad \text{and} \qquad [\langle n\rangle] = n+1.$$

Definition 2.3: A function $f\colon \mathbf{N}_0 \to \mathbf{N}_0$ is *computable* if there exists a Turing machine M such that, for every integer n, M halts on $\langle n\rangle$ and

$$f(n) = [\text{term}(\alpha(\langle n\rangle))]$$

We then say that M *computes* f.

That is, given a function f and an integer n, we input $\langle n\rangle$ and apply M. If M always halts on $\langle n\rangle$ and the number of 1s in the final picture is equal to $f(n)$, then f is a computable function and we say that M computes f.

EXAMPLE 13.15 The function $f(n) = n+3$ is computable. The input is $W = 1^{n+1}$. Thus we need only add two 1s to the input. A Turing machine M which computes f follows:

$$M = \{q_1, q_2, q_3\} = \{s_0 11 s_0 L,\ s_0 B 1 s_1 L,\ s_1 B 1 s_H N\}$$

Observe that:

(1) q_1 moves the machine M to the left.
(2) q_2 writes 1 in the blank square B, and moves M to the left.
(3) q_3 writes 1 in the blank square B, and halts M.

Accordingly, for any positive integer n,

$$s_0 1^{n+1} \to s_0 B 1^{n+1} \to s_1 B 1^{n+2} \to s_H 1^{n+3}$$

Thus M computes $f(n) = n+3$. It is clear that, for any positive integer k, the function $f(n) = n+k$ is computable.

The following theorem applies.

Theorem 13.8: Suppose $f\colon \mathbf{N}_0 \to \mathbf{N}_0$ and $g\colon \mathbf{N}_0 \to \mathbf{N}_0$ are computable. Then the composition function $h = g \circ f$ is computable.

We indicate the proof of this theorem here. Suppose M_f and M_g are the Turing machines which compute f and g, respectively. Given the input $\langle n\rangle$, we apply M_f to $\langle n\rangle$ to finally obtain an expression E with $[E] = f(n)$. We then arrange that $E = s_0 1^{f(n)}$. We next add 1 to E to obtain $E' = s_0 11^{f(n)}$ and apply M_g to E'. This yields E'' where $[E''] = g(f(n)) = (g \circ f)(n)$, as required.

Functions of Several Variables

This subsection defines a conputable function $f(n_1, n_2, \ldots, n_k)$ of k variables. First we need to represent the list $m = (n_1, n_2, \ldots, n_k)$ in our alphabet A.

Definition 2.4: Each list $m = (n_1, n_2, \ldots, n_k)$ of k integers is represented by the tape expression $\langle m\rangle$ where

$$\langle m\rangle = \langle n_1\rangle B\langle n_2\rangle B \cdots B\langle n_k\rangle$$

Thus $\langle (2, 0, 4)\rangle = 111B1B11111 = 1^3B1^1B1^5$.

Definition 2.5: A function $f(n_1, n_2, \ldots, n_k)$ of k variables is computable if there is a Turing machine M such that, for every list $m = (n_1, n_2, \ldots, n_k)$, M halts on $\langle m\rangle$ and

$$f(m) = [\text{term}(\alpha(\langle m\rangle))]$$

We then say that M *computes* f.

The definition is analogous to Definition 2.3 for one variable.

EXAMPLE 13.16 The addition function $f(m,n) = m + n$ is computable. The input is $W = 1^{m+1}B1^{n+1}$. Thus we need only erase two of the 1s. A Turing machine M which computes f follows:

$$M = \{q_1, q_2, q_3, q_4\} = \{s_0\,1Bs_1R,\ s_1\,1Bs_HN,\ s_1BBs_2,\ s_2\,1Bs_HN\}$$

Observe that:

(1) q_1 erases the first 1 and moves M to the right.
(2) If $m \neq 0$, then q_2 erases the second 1 and halts M.
(3) If $m \neq 0$, q_3 moves M to the right past the blank space B.
(4) q_4 erases the 1 and halts M.

Accordingly, if $m \neq 0$ we have:

$$s_0 1^{m+1}B1^{n+1} \rightarrow s_1 1^m B1^{n+1} \rightarrow s_H 1^{m-1}B1^{n+1}$$

but if $m = 0$ and $m + n = n$, we have

$$s_0 1B1^{n+1} \rightarrow s_1 B1^{n+1} \rightarrow s_2 1^{n+1} \rightarrow s_H 1^n$$

Thus M computes $f(m,n) = m + n$.

Solved Problems

WORDS

13.1. Consider the words $u = a^2ba^3b^2$ and $v = bab^2$. Find: (*a*) uv; (*b*) vu; (*c*) v^2.

Write the letters of the first word followed by the letters of the second word:

(*a*) $uv = (a^2ba^3b^2)(bab^2) = a^2ba^3b^3ab^2$.
(*b*) $vu = (bab^2)(a^2ba^3b^2) = bab^2a^2ba^3b^2$.
(*c*) $v^2 = vv = (bab^2)(bab^2) = bab^3ab^2$.

13.2. Find $|u|$, $|v|$, $|uv|$, $|vu|$, $|v^2|$ for the words u and v in Problem 13.1.

Count the number of letters in each word to obtain:

$$|u| = 8, \qquad |v| = 4, \qquad |uv| = 12, \qquad |vu| = 12, \qquad |v^2| = 8$$

13.3. Suppose $u = a^2b$ and $v = b^3ab$. Find: (*a*) uvu; (*b*) λu, $u\lambda$, $u\lambda v$.

(*a*) Write down the letters in u, then v, and finally u to obtain $uvu = a^2b^4aba^2b$.
(*b*) Since λ is the empty word, $\lambda u = u\lambda = u = a^2b$ and $u\lambda v = uv = a^2b^4ab$.

13.4. Let $w = abcd$. (*a*) Find all subwords of w. (*b*) Which of them are initial segments?

(*a*) The subwords are:

$$\lambda, \quad a, \quad b, \quad c, \quad d, \quad ab, \quad bc, \quad cd, \quad abc, \quad bcd, \quad w = abcd$$

We emphasize that $v = acd$ is not a subword of w even though all its letters belong to w.

(*b*) The initial segments are λ, a, ab, abc, $w = abcd$.

13.5. For any words u and v, show that: (*a*) $|uv| = |u| + |v|$; (*b*) $|uv| = |vu|$.

(*a*) Suppose $|u| = r$ and $|v| = s$. Then uv will consist of the r letters of u followed by the s letters of v; hence $|uv| = r + s = |u| + |v|$.

(*b*) Using (*a*) yields $|uv| = |u| + |v| = |v| + |u| = |vu|$.

13.6. Suppose $|u| = n$. Find the number of initial segments of u.

Say $u = a_1 a_2 \cdots a_n$. Then there are $n + 1$ initial segments: $u_k = a_1 a_2 \cdots a_k$, for $k = 1, 2, \ldots, n$, and λ.

13.7. What, if any, is the difference between the free semigroup on an alphabet A and the free monoid on A?

The free semigroup on A is the set of all nonempty words in A under the operation of concantenation; it does not include the empty word λ. On the other hand, the free monoid on A does include the empty word λ.

LANGUAGES

13.8. Let $A = \{a, b\}$. Describe verbally the following languages over A (which are subsets of A^*):

(*a*) $L_1 = \{(ab)^m : m > 0\}$.

(*b*) $L_2 = \{a^r b a^s b a^t : r, s, t \geq 0\}$.

(*c*) $L_3 = \{a^2 b^m a^3 : m > 0\}$.

(*a*) L_1 consists of words $w = ababab \cdots ab$, that is, beginning with a, alternating with b, and ending with b.

(*b*) L_2 consists of all words with exactly two b's.

(*c*) L_3 consists of all words beginning with a^2 and ending with a^3 with one or more b's between them.

13.9. Let $K = \{a, ab, a^2\}$ and $L = \{b^2, aba\}$ be languages over $A = \{a, b\}$. Find: (*a*) KL; (*b*) LL.

(*a*) Concatenate words in K with words in L to obtain $KL = \{ab^2, a^2ba, ab^3, ababa, a^2b^2, a^3ba\}$.

(*b*) Concatenate words in L with words in L to obtain $LL = \{b^4, b^2aba, abab^2, aba^2ba\}$.

13.10. Consider the language $L = \{ab, c\}$ over $A = \{a, b, c\}$. Find: (*a*) L^0; (*b*) L^3; (*c*) L^{-2}.

(*a*) $L^0 = \{\lambda\}$, by definition.

(*b*) Form all three-word sequences from L to obtain

$$L = \{ababab,\ ababc,\ abcab,\ abc^2,\ cabab,\ cabc,\ c^2ab,\ c^3\}$$

(*c*) The negative power of a language is not defined.

13.11. Let $A = \{a, b, c\}$. Find L^* where: (*a*) $L = \{b^2\}$; (*b*) $L = \{a, b\}$; (*c*) $L = \{a, b, c^3\}$.

(*a*) L^* consists of all words b^n where n is even (including the empty word λ).

(*b*) L^* consists of words in a and b.

(*c*) L^* consists of all words from A with the property that the length of each *maximal* subword composed entirely of c's is divisible by 3.

13.12. Consider a countable alphabet $A = \{a_1, a_2, \ldots\}$. Let L_k be the language over A consisting of those words w such that the sum of the subscripts of the letters in w is equal to k. For example, $w = a_2a_3a_3a_6a_4$ belongs to L_{18}. (*a*) Find L_4. (*b*) Show that L_k is finite. (*c*) Show that A^* is countable. (*d*) Show that any language over A is countable.

(*a*) No letter a_n with $n > 4$ can be used in L_4. Also, no word in L_4 can have more than four letters. Thus we obtain the following list:

$$a_1a_1a_1a_1, \quad a_1a_1a_2, \quad a_1a_2a_1, \quad a_2a_1a_1, \quad a_1a_3, \quad a_3a_1, \quad a_2a_2, \quad a_4$$

(*b*) Only a finite number of the a's that is, $a_1, a_2, \ldots, a_k$, can be used in L_k and no word in L_k can have more than k letters. Thus L_k is finite.

(*c*) A^* is the countable union of the finite sets L_k; hence A^* is countable.

(*d*) L is a subset of the countable set A^*; hence L is also countable.

REGULAR EXPRESSIONS, REGULAR LANGUAGES

13.13. Let $A = \{a, b, c\}$. Describe the language $L(r)$ for each regular expression:

(*a*) $r = ab^*c^*$; (*b*) $r = a^* \vee b^* \vee c^*$.

$L(r)$ consists of all words w in a, b, c such that:

(*a*) w contains exactly one a which is the first letter;

(*b*) w is a word only in a or only in b or only in c, that is,

$$L(r) = \{\lambda, a, a^2, \ldots, b, b^2, \ldots, c, c^2, \ldots\}$$

13.14. Let $A = \{a, b\}$. Describe the language $L(r)$ where:

(*a*) $r = abb^*a$; (*b*) $r = b^*ab^*ab^*$; (*c*) $r = ab^* \wedge a^*$.

(*a*) $L(r)$ consists of all words beginning and ending in a and enclosing one or more b's.

(*b*) $L(r)$ consists of all words with exactly two a's.

(*c*) Here r is not a regular expression since $\wedge$ is not one of the symbols adjoined to A for forming regular expressions.

13.15. Let $A = \{a, b, c\}$ and let $w = ac$. State whether or not w belongs to $L(r)$ where:
(*a*) $r = ab^*c^*$; (*b*) $r = (a^*b \vee c)^*$.

(*a*) Yes, since $w = a\lambda c$ and $\lambda \in L(b^*)$ and $c \in L(c^*)$.

(*b*) No. Note $L(a^*b)$ consists of words a^nb. Thus if a appears in a word in $L(r)$, then a can only be followed by an a or b, not by c.

13.16. Let $A = \{a, b, c\}$ and let $w = abc$. State whether or not w belongs to $L(r)$ where:
(*a*) $r = a^* \vee (b \vee c)^*$; (*b*) $r = a^*(b \vee c)^*$.

(*a*) No. Here $L(r)$ consists of word in a or words in b and c.

(*b*) Yes, since $a \in L(a^*)$ and $bc \in (b \vee c)^*$.

13.17. Let $A = \{a, b\}$. Find a regular expression r such that $L(r)$ consists of all words w where:
(*a*) w begins with a^2 and ends with b^2; (*b*) w contains an even number of a's.

(*a*) Let $r = a^2(a \vee b)^*b^2$.

(*b*) Note $s = b^*ab^*ab^*$ consists of all words with exactly two a's. Then let $r = s^* = (b^*ab^*ab^*)^*$.

FINITE AUTOMATA, FINITE STATE MACHINES

13.18. Let M be the automaton with the following input set A, state set S, and accepting (''yes'') state set Y:

$$A = \{a, b\}, \qquad S = \{s_0, s_1, s_2\}, \qquad Y = \{s_1\}$$

Suppose s_0 is the initial state of M, and next state function F of M is given by the table in Fig. 13-10(*a*).

(*a*) Draw the state diagram $D = D(M)$ of M.

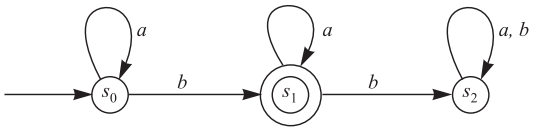
(*b*) Describe the language $L = L(M)$ accepted by M.

(*a*) The state diagram D appears in Fig. 13-10(*b*). The vertices of D are the states with a double circle indicating an accepting state. If $F(s_j, x) = s_k$, then there is a directed edge from s_j to s_k labeled by the input symbol x. Also, there is a special arrow which terminates at the initial state s_0.

(*b*) $L(M)$ consists of all words w with exactly one b. Specifically, if an input word w has no b's, then it terminates in s_0 and if w has two or more b's then it terminates in s_2. Otherwise w terminates in s_1, which is the only accepting state.

F	a	b
s_0	s_0	s_1
s_1	s_1	s_2
s_2	s_2	s_2

(*a*)



(*b*)

Fig. 13-10

13.19. Let $A = \{a, b\}$. Construct an automaton M which will accept precisely those words from A which have an even number of a's. For example, *aababbab*, *aa*, *bbb*, *ababaa* will be accepted by M, but *ababa*, *aaa*, *bbabb* will be rejected by M.

We need only two states, s_0 and s_1. We assume that M is in state s_0 or s_1 according as the number of a's up to the given step is even or odd. (Thus s_0 is an accepting state, but s_1 is a rejecting state.) Then only a will change the state. Also, s_0 is the initial state. The state diagram of M is shown in Fig. 13-11.

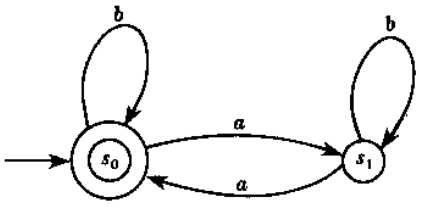


Fig. 13-11

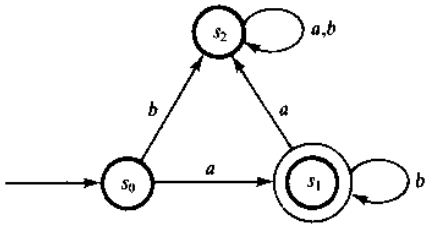


Fig. 13-12

13.20. Let $A = \{a, b\}$. Construct an automaton M which will accept those words from A which begin with an a followed by (zero or more) b's.

See Fig. 13-12.

13.21. Describe the words w in the language L accepted by the automaton M in Fig. 13-13.

The system can reach the accepting state s_2 only when there exists an a in w which follows a b.

13.22. Describe the words w in the language L accepted by the automaton M in Fig. 13-14.

Each a in w does not change the state of the system, whereas each b in w changes the state from s_i to s_{i+1} (modulo 4). Thus w is accepted by M if the number n of b's in w is congruent to 3 modulo 4, that is, where $n = 3, 7, 11, \ldots$.

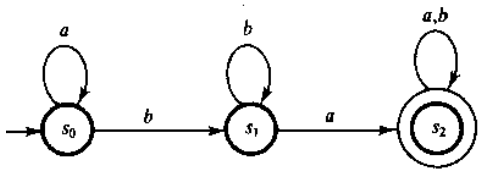


Fig. 13-13

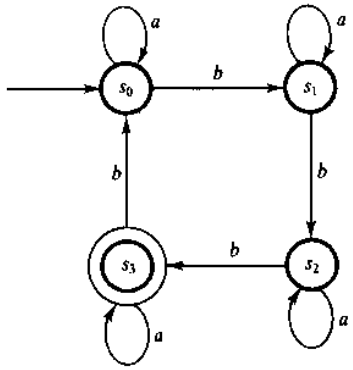


Fig. 13-14

13.23. Suppose L is a language over A which is accepted by the automaton $M = \langle A, S, Y, s_0, F\rangle$. Find an automaton N which accepts L^c, that is, those words from A which do not belong to L.

Simply interchange the accepting and rejecting states in M to obtain N. Then w will be accepted in the new machine N if and only if w is rejected in M, i.e., if and only if w belongs to L^c. Formally, $N = \langle A, S, S\backslash Y, s_0, F\rangle$.

13.24. Let $M = \langle A, S, Y, s_0, F\rangle$ and $M' = \langle A, S', Y', s_0', F'\rangle$ be automata over the same alphabet A which accept the languages $L(M)$ and $L(M')$ over A, respectively. Construct an automaton N over A which accepts precisely $L(M) \cap L(M')$.

Let $S \times S'$ be the set of states of N. Let (s, s') be an accepting state of N if s and s' are accepting states in M and M', respectively; and let (s_0, s_0') be the initial state of N. The next-state function of N, $G: (S \times S') \times A \to (S \times S')$, defined as

$$G((s, s'), a) = (F(s, a), F'(s', a))$$

Then N will accept precisely those words in $L(M) \cap L(M')$.

13.25. Repeat Problem 13.24 except now let N accept precisely $L(M) \cup L(M')$.

Again, let $S \times S'$ be the set of states of N and let (s_0, s_0') be the initial state of N. Now let $(S \times Y') \cup (Y \times S')$ be the accepting states in N. The next-state function G is again defined by

$$G((s, s'), a) = (F(s, a), F'(s', a))$$

Then N will accept precisely those words in $L(M) \cup L(M')$.

13.26. Let M be the finite state machine with state table appearing in Fig. 13-15(a).

(a) Find the input set A, the state set S, the output set Z, and the initial state.

(b) Draw the state diagram $D = D(M)$ of M.

(c) Suppose $w = aababaabbab$ is an input word (string). Find the corresponding output word v.

(*a*) The input symbols are on the top of the table, the states are listed on the left, and the output symbols appear in the table. Thus:

$$A = \{a, b\} \qquad S = \{s_0, s_1, s_2, s_3\}, \qquad Z = \{x, y, z\}$$

The state s_0 is the initial state since it is the first state listed in the table.

(*b*) The state diagram $D = D(M)$ appears in Fig. 13-15(*b*). Note that the vertices of D are the states of M. Suppose

$$F(s_i, a_j) = (s_k, z_r), \qquad \text{that is,} \qquad f(s_i, a_j) = s_k \qquad \text{and} \qquad g(s_i, a_j) = z_r$$

Then there is a directed edge from s_i to s_k labeled by the pair a_j, z_r. Usually, the input symbol a_j is put near the base of the arrow (near s_i) and output symbol z_r is put near the center of the arrow.

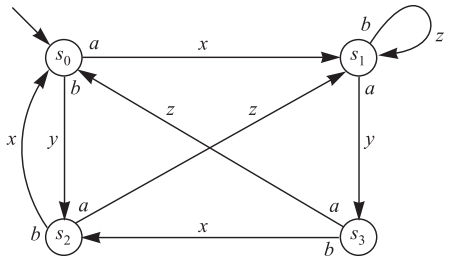
(*c*) Starting at the initial state s_0, we move from state to state by the arrows which are labeled, respectively, by the given input symbols as follows:

$$s_0 \xrightarrow{a} s_1 \xrightarrow{a} s_3 \xrightarrow{b} s_2 \xrightarrow{a} s_1 \xrightarrow{b} s_1 \xrightarrow{a} s_3 \xrightarrow{a} s_0 \xrightarrow{b} s_2 \xrightarrow{b} s_0 \xrightarrow{a} s_1 \xrightarrow{b} s_1$$

The output symbols on the above arrows yield the required output word $v = xyxzzyzyxxz$.

F	a	b
s_0	s_1, x	s_2, y
s_1	s_3, y	s_1, z
s_2	s_1, z	s_0, x
s_3	s_0, z	s_2, x

(*a*)



(*b*)

Fig. 13-15

GRAMMARS

13.27. Define: (*a*) context-free grammar; (*b*) regular grammar.

(*a*) A context-free grammar is the same as a Type 2 grammar, that is, every production is of the form $A \to \beta$, that is, the left side is a single variable and the right side is a word in one or more symbols.

(*b*) A regular grammar is the same as a Type 3 grammar, that is, every production is of the form $A \to a$ or $A \to aB$, that is, the left side is a single variable and the right side is either a single terminal or a terminal followed by a variable.

13.28. Find the language $L(G)$ generated by the grammar G with variables S, A, B, terminals a, b, and productions $S \to aB$, $B \to b$, $B \to bA$, $A \to aB$.

Observe that we can only use the first production once since the start symbol S does not appear anywhere else. Also, we can only obtain a terminal word by finally using the second production. Otherwise we alternately add a's and b's using the third and fourth productions. In other words,

$$L(G) = \{(ab)^n = ababab \cdots ab : n \in \mathbf{N}\}$$

13.29. Let L be the set of all words in a and b with an even number of a's. Find a grammar G which will generate L.

We claim that the grammar G with the following productions will generate L:

$$S \to aA, \qquad S \to bB, \qquad B \to bB, \qquad B \to aA, \qquad A \to aB, \qquad A \to bA, \qquad A \to a, \qquad B \to b$$

Observe that the sum of the a's and A's in any word α either remains the same or is increased by 2 when any production is applied to α. Thus any word w in the terminals a and b which is derived from S must contain an even number of a's. In other words $L(G) \subseteq L$. On the other hand, it is clear which productions should be used to print any word v in L; that is, we use $S \to aA$ or $S \to bB$ according as v begins with a or b, and we use $A \to aB$ or $B \to aA$ if any subsequent letter is an a, and we use $A \to bA$ or $B \to bB$ if any subsequent letter is a b. For the last letter of v we use $A \to a$ or $B \to b$. Thus $L(G) = L$.

13.30. Determine the type of grammar G which consists of the productions:

(*a*) $S \to aA,\ A \to aAB,\ B \to b,\ A \to a.$

(*b*) $S \to aAB,\ AB \to bB,\ B \to b,\ A \to aB.$

(*c*) $S \to aAB,\ AB \to a,\ A \to b,\ B \to AB.$

(*d*) $S \to aB,\ B \to bA,\ B \to b,\ B \to a,\ A \to aB,\ A \to a.$

(*a*) Each production is of the form $A \to \alpha$, i.e., a variable on the left; hence G is a context-free or Type 2 grammar.

(*b*) The length of the left side of each production does not exceed the length of the right side; hence G is a Type 1 grammar.

(*c*) The production $AB \to a$ means G is a Type 0 grammar.

(*d*) G is a regular or Type 3 grammar since each production has the form $A \to a$ or $A \to aB$.

13.31. Let L be the language on $A = \{a, b\}$ which consists of all words w with exactly one b, that is,

$$L = \{b, a^r b,\ ba^s,\ a^r ba^s : r > 0,\ s > 0\}.$$

(*a*) Find a regular expression r such that $L = L(r)$.

(*b*) Find a regular grammar G which generates the language L.

(*a*) Let $r = a^* ba^*$. Then $L(r) = L$.

(*b*) The regular grammar G with the following productions generates L:

$$S \to (b, aA), \qquad A \to (b, aA, bB), \qquad B \to (a, aB)$$

That is, the letter b can only appear once in any word derived from S. G is regular since it has the required form.

13.32. Let L be the language on $A = \{a, b, c\}$ which consists of all words of the form $w = a^r b^s c^t$ where $r, s, t > 0$, that is, a's followed by b's followed by c's.

(*a*) Find a regular expression r such that $L = L(r)$.

(*b*) Find a regular grammar G which generates the language L.

(*a*) Let $r = aa^* bb^* cc^*$. Then $L = L(r)$.

(*b*) The regular grammar G with the following productions generates L:

$$S \to aA, \qquad A \to (aA, bB), \qquad B \to (bB, c, cC), \qquad C \to (c, cC)$$

13.33. Consider the regular grammar G with productions

$$S \to aA, \qquad A \to aB, \qquad B \to bB, \qquad B \to a$$

(*a*) Find the derivation tree of the word $w = aaba$.

(*b*) Describe all words w in the language L generated by G.

(*a*) Note first that w can be derived from S as follows:

$$S \Rightarrow aA \Rightarrow a(aB) \Rightarrow aa(bB) \Rightarrow aaba$$

Figure 13-16 shows the corresponding derivation tree.

(*b*) Using the production 1, then 2, then 3, r times, and 4 will derive the word $w = aab^r a$ where $r \geq 0$. No other word can be derived from S.

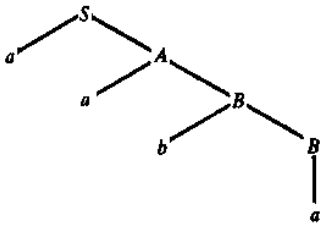


Fig. 13-16

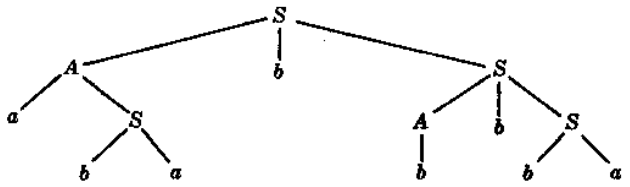


Fig. 13-17

13.34. Figure 13-17 is the derivation tree of a word w in the language L of a context-free grammar G. (*a*) Find w. (*b*) Which terminals, variables, and productions must lie in G?

(*a*) The sequence of leaves from left to right yields the word $w = ababbbba$.

(*b*) The leaves show that a and b must be terminals, and the internal vertices show that S and A must be variables with S the starting variable. The children of each variable show that $S \to AbS$, $A \to aS$, $S \to ba$, and $A \to b$ must be productions.

13.35. Does a derivation tree exist for any word w derived from the start symbol S in a grammar G?

No. Derivation trees only exist for Type 2 and 3 grammars, that is, for context-free and regular grammars.

13.36. Rewrite each grammar G in Problems 13.30 in Backus-Naur form.

The Backus-Naur form only applies to context-free grammars (which includes regular grammars). Thus only (*a*) and (*d*) can be written in Backus-Naur form. The form is obtained as follows:

(i) Replace $\to$ by $::=$.

(ii) Enclose nonterminals in brackets $\langle\ \rangle$.

(iii) All productions with the same left-hand side are combined in one statement with all the right-hand sides listed on the right of $::=$ separated by vertical bars.

Accordingly:

(*a*) $\langle S\rangle ::= a\langle A\rangle,\ \langle A\rangle ::= a\langle A\rangle\langle B\rangle | a,\ \langle B\rangle ::= b.$

(*d*) $\langle S\rangle ::= a\langle B\rangle,\ \langle B\rangle ::= b\langle A\rangle | b | a,\ \langle A\rangle ::= a\langle B\rangle | a.$

TURING MACHINES

13.37. Let M be a Turing machine. Determine the picture α corresponding to each situation:

(*a*) M is in state s_3 and scanning the third letter of the tape expression $w = aabca$.

(*b*) M is in state s_2 and scanning the last letter of the tape expression $w = abca$.

(*c*) The input is the tape expression $w = 1^4B1^2$.

The picture α is obtained by placing the state symbol before the tape letter being scanned. Initially, M is in state s_0 scanning the first letter of an input. Thus:

(*a*) $\alpha = aas_3bca$ (*b*) $\alpha = abcs_2a$; (*c*) $\alpha = s_0 1111B11$.

13.38. Suppose $\alpha = aas_2ba$ is a picture. Find β such that $\alpha \to \beta$ if the Turing machine M has the quintuple q where:

(*a*) $q = s_2bas_1L$; (*b*) $q = s_2bbs_3R$; (*c*) $q = s_2bas_2N$; (*d*) $q = s_3abs_1L$.

(*a*) Here M erases b and writes a, changes its state to s_1, and moves left. Thus $\beta = as_1aaa$.

(*b*) Here M does not change the scanned letter b, changes its state to s_3, and moves right. Thus $\beta = aabs_3a$.

(*c*) Here M erases b and writes a, keeps its state s_2, and does not move. Thus $\beta = aas_2aa$.

(*d*) Here q has no effect on α since q does not begin with s_2b.

13.39. Let $A = \{a, b\}$ and let $L = \{a^r b^s : r > 0, s > 0\}$, that is, L consists of all words W beginning with one or more a's and followed by one or more b's. Find a Turing machine M which recognizes L.

The strategy is that we want M to (1) move right over all the a's, (2) move right over the b's, and (3) halt in the accepting state s_Y when it meets the blank symbol B. The following quintuples do this:

$$q_1 = s_0aas_1R, \qquad q_2 = s_1aas_1R, \qquad q_3 = s_1bbs_2R, \qquad q_4 = s_2bbs_2R, \qquad q_5 = s_2BBs_YR$$

Specifically, q_1 and q_2 do (1), q_3 and q_4 do (2), and q_5 does (3).

However, we also want M to nonaccept an input word W which does not belong to L. Thus we also need the quintuples

$$q_6 = s_0BBs_NR, \qquad q_7 = s_0bbs_NR, \qquad q_8 = s_1BBs_NR, \qquad q_9 = s_2aas_NR$$

Note that q_6 is used if the input $W = \lambda = B$, the empty word; q_7 is used if the input W is an expression beginning with b; q_8 is used if the input W only contains a's; and q_9 is used if the input W contains the letter a following a letter b.

13.40. Find a Turing machine M which recognizes the language $L = (ab)^* = \{(ab)^n : n \geq 0\}$.

Given an input W, the strategy is to have M erase the first a, the last b, the first a, the last b, and so on. If all the letters are erased, then M accepts W since W belongs to L. Otherwise, we want M to nonaccept (reject) W. Accordingly, M will need the following 17 quintuples:

(1) M in the initial state s_0 erases the first a and enters state s_1, or M accepts W if $W = \lambda$ or rejects W if W begins with b:.

$$q_1 = s_0aBs_1R, \qquad q_2 = s_0BBs_YR, \qquad q_3 = s_0bbs_NR$$

(2) M in state s_1 moves rightward through the a's until M either meets b and enters state s_2, or M rejects W if there is no b:

$$q_4 = s_1aas_1R, \qquad q_5 = s_1bbs_2R, \qquad q_6 = s_1BBs_NR$$

(3) M in state s_2 moves rightward through the b's until M either meets B and then enters state s_3 and moves left, or M rejects W if M meets an a:

$$q_7 = s_2bbs_2R, \qquad q_8 = s_2BBs_3L, \qquad q_9 = s_2aas_NR$$

(4) M in state s_3 erases the last b and then enters state s_4 and moves left:

$$q_{10} = s_3bBs_4L$$

(5) M in s_4 halts in state s_Y (success) if M meets B, or M moves left past the rightmost b in state s_5:

$$q_{11} = s_4BBs_YL, \qquad q_{12} = s_4bbs_5L$$

(6) M in state s_5 moves leftward through the b's until M either meets a or rejects W if there is a B:

$$q_{13} = s_5bbs_5L, \qquad q_{14} = s_5aas_6L, \qquad q_{15} = s_5BBs_NL$$

(7) M in state s_6 moves leftward through the a's and returns to the initial state s_0 when meeting B:

$$q_{16} = s_6aas_6L, \qquad q_{17} = s_6BBs_0R$$

COMPUTABLE FUNCTIONS

13.41. Find $\langle m \rangle$ if: (*a*) $m = 5$; (*b*) $m = (4, 0, 3)$; (*c*) $m = (3, -2, 5)$.

Recall $\langle n \rangle = 1^{n+1} = 11^n$ and $\langle (n_1, n_2, \ldots, n_r) \rangle = \langle n_1 \rangle B \langle n_2 \rangle B \cdots B \langle n_r \rangle$. Thus:

(*a*) $\langle m \rangle = 1^6 = 111111$.

(*b*) $\langle m \rangle = 1^5 B 1^1 B 1^4 = 11111B1B1111$.

(*c*) $\langle m \rangle$ is not defined for negative integers.

13.42. Find $[E]$ for the expressions:

(*a*) $E = a11s_2Bb111$.

(*b*) $E = aas_3bb$.

(*c*) $E = \langle m \rangle$ where $m = (4, 1, 2)$.

(*d*) $E = \langle m \rangle$ where $m = (n_1, n_2, \ldots, n_r)$.

Recall that $[E]$ counts the number of 1s in E. Thus:

(*a*) $[E] = 5$.

(*b*) $[E] = 0$.

(*c*) $[E] = 10$ since $E = 1^5 B 1^2 B 1^3$.

(*d*) $[E] = n_1 + n_2 + \cdots + n_r + r$ since the number of 1s contributed by each n_k to E is $n_k + 1$.

13.43. Let f be the function $f(n) = n - 1$ when $n > 0$ and $f(0) = 0$. Show that f is computable.

We need to find a Turing machine M which computes f. Specifically, we want M to erase two of the 1s in the input $\langle n \rangle$ when $n > 0$, but only one 1 when $n = 0$. This is accomplished with the following quintuples:

$$q_1 = s_0 1 B s_1 R, \qquad q_2 = s_1 B B s_H N, \qquad q_3 = s_1 1 B s_H N$$

Here q_1 erases the first 1 and moves M right. If there is only one 1, then M is now scanning a blank symbol B and q_2 tells the computer to halt. Otherwise, q_3 erases the second 1 and halts M.

13.44. Let f be the function $f(x, y) = y$. Show that f is computable.

We need to find a Turing machine M which computes f. Specifically, we want M to erase all the 1s from $\langle x \rangle$ and one of the 1s from $\langle y \rangle$. This is accomplished with the following quintuples:

$$q_1 = s_0 1 B s_0 R, \qquad q_2 = s_0 B B s_1 R, \qquad q_3 = s_1 1 B s_H N$$

Here q_1 erases all the 1s in $\langle x \rangle$ while moving M to the right. When M scans the diving blank B, q_2 changes the state of M from s_0 to s_1 and moves M right. Then q_3 erases the first 1 in $\langle y \rangle$ and halts M.

Supplementary Problems

WORDS

13.45. Consider the words $u = ab^2a^3$ and $v = aba^2b^2$. Find: (*a*) uv; (*b*) vu; (*c*) u^2; (*d*) λu; (*e*) $v\lambda v$.

13.46. For the words $u = ab^2a^3$ and $v = aba^2b^2$, find: $|u|$, $|v|$, $|uv|$, $|vu|$, and $|v^2|$.

13.47. Let $w = abcde$. (*a*) Find all subwords of w. (*b*) Which of them are initial segments?

13.48. Suppose $u = a_1a_2 \cdots a_r$, and the a_k are distinct. Find the number n of subwords of u.

LANGUAGES

13.49. Let $L = \{a^2, ab\}$ and $K = \{a, ab, b^2\}$. Find: (*a*) LK; (*b*) KL; (*c*) $L \vee K$; (*d*) $K \vee L$.

13.50. Let $L = \{a^2, ab\}$. Find: (*a*) L^0; (*b*) L^2; (*c*) L^3.

13.51. Let $A = \{a, b, c\}$. Describe L^* if: (*a*) $L = \{a^2\}$; (*b*) $L = \{a, b^2\}$; (*c*) $L = \{a, b^2, c^3\}$.

13.52. Does $(L^2)^* = (L^*)^2$? If not, how are they related?

13.53. Consider a countable alphabet $A = \{a_1, a_2, \ldots\}$. Let L_k be the language over A consisting of those words w such that the sum of the subscripts of the letters in w is equal to k. (See Problem 13.12.) Find:
(*a*) L_3; (*b*) L_5.

REGULAR EXPRESSIONS, REGULAR LANGUAGES

13.54. Let $A = \{a, b, c\}$. Describe the language $L(r)$ for each regular expression:
(*a*) $r = ab^*c$; (*b*) $r = (ab \vee c)^*$; (*c*) $r = ab \vee c^*$.

13.55. Let $A = \{a, b\}$. Find a regular expression r such that $L(r)$ consists of all words w where:

(*a*) w contains exactly three a's.

(*b*) The number of a's is divisible by 3.

(*c*) w begins and ends in b, and bab is never a subword of w; i.e., wherever a occurs in w, its exponent is 2 or more.

13.56. Let $A = \{a, b, c\}$ and let $w = ac$. State whether or not w belongs to $L(r)$ where:
(*a*) $r = a^*bc^*$; (*b*) $r = a^*b^*c$; (*c*) $r = (ab \vee c)^*$.

13.57. Let $A = \{a, b, c\}$ and let $w = abc$. State whether or not w belongs to $L(r)$ where:
(*a*) $r = ab^*(bc)^*$; (*b*) $r = a^* \vee (b \vee c)^*$; (*c*) $a^*b(bc \vee c^2)^*$.

FINITE AUTOMATA

13.58. Let $A = \{a, b\}$. Construct an automaton M such that $L(M)$ will consist of those words where the number of b's is divisible by 3. (Hint: Three states are needed.)

13.59. Let $A = \{a, b\}$. Construct an automaton M such that $L(M)$ will consist of those words w which begin with a and end in b.

13.60. Let $A = \{a, b\}$. Construct an automaton M which will accept the language $L(M) = \{a^r b^s : r > 0, s > 0\}$.

13.61. Let $A = \{a, b\}$. Construct an automaton M which will accept the language $L(M) = \{b^r ab^s : r > 0, s > 0\}$.

13.62. Let $A = \{a, b\}$. Construct the automaton M such that $L(M)$ will consist of those words where the number of a's is divisible by 2 and the number of b's is divisible by 3. (Hint: Use Problems 13.19, 13.58, and 13.24.)

13.63. Find the language $L(M)$ accepted by the automaton M in Fig. 13-18.

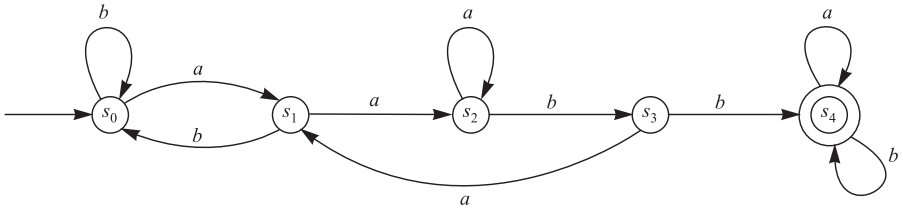


Fig. 13-18

FINITE STATE MACHINES

13.64. Let M be the finite state machine with state table appearing in Fig. 13-19.

(*a*) Find the input set A, the state set S, the output set Z, and the initial state of M.

(*b*) Draw the state diagram $D = D(M)$ of M.

(*c*) Find the output word v if the input is the word $w = a^2b^2ab^2a^2b$.

F	a	b
s_0	s_2, y	s_1, z
s_1	s_2, x	s_3, y
s_2	s_2, y	s_1, z
s_3	s_3, z	s_0, x

Fig. 13-19

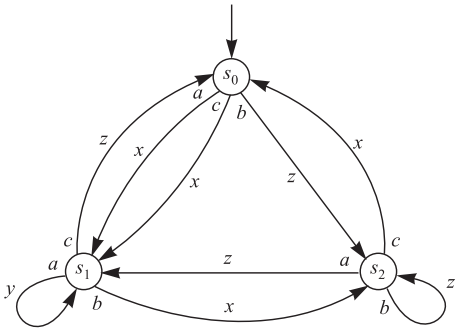


Fig. 13-20

13.65. Let M be the finite state machine with input set $A = \{a, b, c\}$, output set $Z = \{x, y, z\}$ and state diagram $D = D(M)$ in Fig. 13-20. (*a*) Construct the state table of M. (*b*) Find the output word v if the input is the word $w = ca^2b^2ac^2ab$.

13.66. For each machine in Fig. 13-21 with input set $A = \{a, b\}$ and output set $Z = \{x, y, z\}$, find the output word v if the input is the word $w = aba^2b^2ab^2a^2ba^2$.

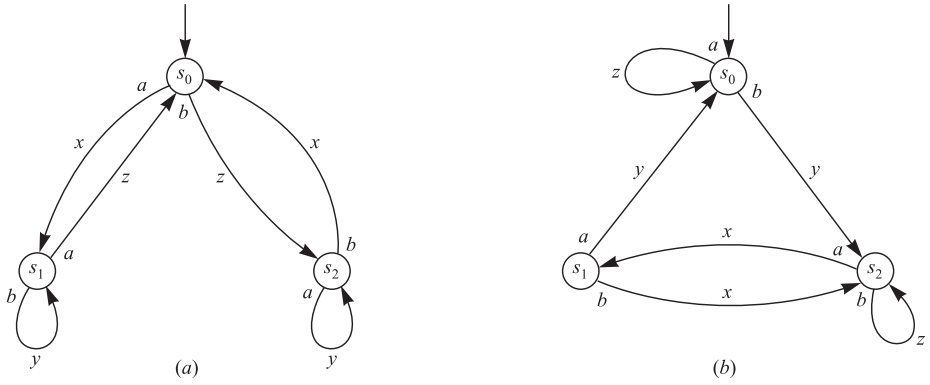


Fig. 13-21

GRAMMARS

13.67. Determine the type of grammar G which consists of the productions:

(*a*) $S \to aAB$; $S \to AB$; $A \to a$; $B \to b$.

(*b*) $S \to aB$; $B \to AB$; $aA \to b$; $A \to a$; $B \to b$.

(*c*) $S \to aB$; $B \to bB$; $B \to bA$; $A \to a$; $B \to b$.

13.68. Find a regular grammar G which generates the language L which consists of all words in a and b such that no two a's appear next to each other.

13.69. Find a context-free grammar G which generates the language L which consists of all words in a and b with twice as many a's as b's.

13.70. Find a grammar G which generates the language L which consists of all words of the form $a^n b a^n$ with $n \geq 0$.

13.71. Show that the language G in Problem 13.70 is not regular. (Hint: Use the Pumping Lemma.)

13.72. Describe the language $L = L(G)$ where G has the productions $S \to aA$, $A \to bbA$, $A \to c$.

13.73. Describe the language $L = L(G)$ where G has the productions $S \to aSb$, $Sb \to bA$, $abA \to c$.

13.74. Write each grammar G in Problem 13.67 in Backus-Naur form.

13.75. Let G be the context-free grammar with productions $S \to (a, aAS)$ and $A \to bS$. (*a*) Write G in Backus-Naur form. (*b*) Find the derivation tree of the word $w = abaabaa$.

13.76. Figure 13-22 is the derivation tree of a word w in a language L of a context-free grammar G. (*a*) Find w. (*b*) Which terminals, variables, and productions must belong to G?

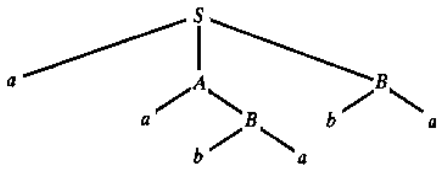


Fig. 13-22

TURING MACHINES

13.77. Let M be a Turing machine. Determine the picture α corresponding to each situation:

(*a*) M is in state s_2 and scanning the third letter of the tape expression $w = abbaa$.

(*b*) M is in state s_3 and scanning the last letter of the tape expression $w = aabb$.

(*c*) The input is the word $W = a^3b^3$.

(*d*) The input is the tape expression $W = \langle (3, 2) \rangle$.

13.78. Suppose $\alpha = abs_2aa$ is a picture. Find β such that $\alpha \to \beta$ if the Turing machine M has the quintuple q where:

(*a*) $q = s_2abs_1R$. (*b*) $q = s_2aas_3L$. (*c*) $q = s_2abs_2N$

(*d*) $q = s_2abs_3L$. (*e*) $q = s_3abs_2R$. (*f*) $q = s_2aas_2N$.

13.79. Repeat Problem 13.78 for the picture $\alpha = s_2aBab$.

13.80. Find distinct pictures α and β and a Turing machine M such that the sequence

$$\alpha \to \beta \to \alpha \to \beta \to \cdots$$

does not terminate.

13.81. Suppose $\alpha \to \beta_1$ and $\alpha \to \beta_2$. Must $\beta_1 = \beta_2$?

13.82. Suppose $\alpha = \alpha(W)$ for some input W, and suppose $\alpha \to \beta \to \alpha$. Can M recognize W?

13.83. Let $A = \{a, b\}$. Find a Turing machine M which recognizes the language $L = \{ab^n : n > 0\}$, that is, where L consists of all words W beginning with one a and followed by one or more b's.

13.84. Let $A = \{a, b\}$. Find a Turing machine M which recognizes the finite language $L = \{a, a^2\}$, that is, where L consists of the first two nonzero powers of a.

COMPUTABLE FUNCTIONS

13.85. Find $\langle m \rangle$ if: (*a*) $m = 6$; (*b*) $m = (5, 0, 3, 1)$; (*c*) $m = (0, 0, 0)$; (*d*) $m = (2, 3, -1)$.

13.86. Find $[E]$ for the expressions: (*a*) $E = 111s_2aa1B111$; (*b*) $E = a11bs_1Bb$; (*c*) $E = \langle m \rangle$ where $m = (2, 5, 4)$.

13.87. Let f be the function $f(n) = n - 2$ when $n > 1$ and $f(n) = 0$ when $n = 0$ or 1. Show that f is computable.

13.88. Let f be the function $f(x, y) = x$. Show that f is computable.

Answers to Supplementary Problems

13.45. (*a*) $uv = ab^2a^4ba^2b^2$; (*b*) $uv = aba^2b^2ab^2a^3$; (*c*) $u^2 = ab^2a^4b^2a^3$; (*d*) $\lambda u = u = ab^2a^3$; (*e*) $v\,\lambda\,v = v^2 = aba^2b^2aba^2b^2$.

13.46. $|u| = 6$; $|v| = 6$; $|uv| = |vu| = 12$; $|v^2| = 12$.

13.47. (*a*) $\lambda,\ a,\ b,\ c,\ d,\ e,\ ab,\ bc,\ cd,\ de,\ abc,\ bcd,\ cde,\ abcd,\ bcde,\ w = abcde$.
(*b*) $\lambda,\ a,\ ab,\ abc,\ abcd,\ w = abcde$.

13.48. If $u \neq \lambda$, then

$$n = 1 + [r + (r-1) + \cdots + 2 + 1] = 1 + r(r+1)/2$$

If $u = \lambda$, then $n = 1$.

13.49. (*a*) $LK = \{a^3,\ a^3b,\ a^2b^2,\ aba,\ abab,\ ab^3\}$.
(*b*) $KL = \{a^3,\ a^2b,\ aba^2,\ abab,\ b^2a^2,\ b^2ab\}$.
(*c*) $L \vee K = \{a^2,\ ab,\ a,\ ab,\ b^2\}$.
(*d*) $K \wedge L$ not defined.

13.50. (*a*) $L^0 = \{\lambda\}$.
(*b*) $L^2 = \{a^4, a^3b, aba^2, abab\}$.
(*c*) $L^3 = \{a^6, a^5b, a^3ba^2, a^3bab, aba^4, aba^3b, ababa^2,\ ababab\}$.

13.51. (*a*) $L^* = \{a^n : n \text{ is even}\}$.
(*b*) All words w in a and b with only even powers of b.
(*c*) All words in a, b, c with each power of b even and each power of c a multiple of 3.

13.52. No. $(L^2)^* \subseteq (L^*)^2$.

13.53. (*a*) $a_1a_1a_1$, a_1a_2, a_2a_1, a_3.
(*b*) $a_1a_1a_1a_1a_1$, $a_1a_1a_1a_2$, $a_1a_1a_2a_1$, $a_1a_2a_1a_1$, $a_2a_1a_1a_1$, $a_1a_1a_3$, $a_1a_3a_1$, $a_3a_1a_1$, a_2a_3, a_3a_2, a_1a_4, a_4a_1, a_5.

13.54. (*a*) $L(r) = \{ab^nc : n \geq 0\}$.
(*b*) All words in x and c where $x = ab$.
(*c*) $L(r) = ab \cup \{c^n : n \geq 0\}$.

13.55. (*a*) $r = b^*ab^*ab^*ab^*$; (*b*) $r = (b^*ab^*ab^*ab^*)^*$ (*c*) $r = bb^*a(a \vee b)^*ab^*b$.

13.56. (*a*) No; (*b*) yes; (*c*) no.

13.57. (*a*) Yes; (*b*) no; (*c*) no.

13.58. See Fig. 13-23.

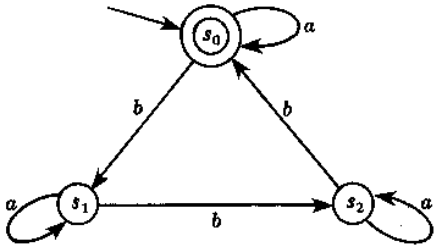


Fig. 13-23

13.59. See Fig. 13-24.

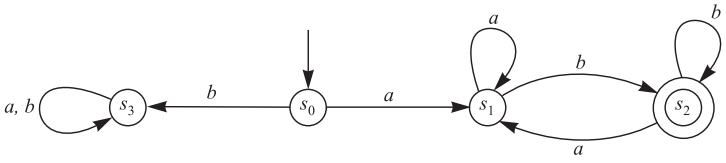


Fig. 13-24

13.60. See Fig. 13-25.

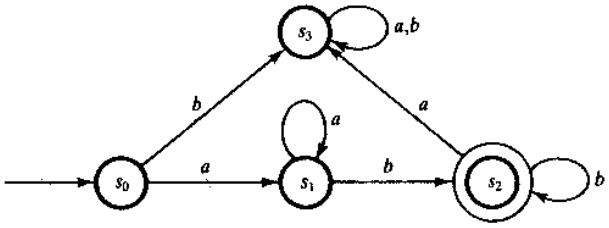


Fig. 13-25

13.61. See Fig. 13-26.

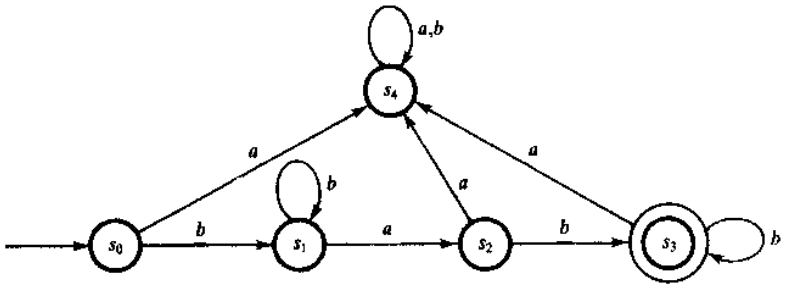


Fig. 13-26

13.62. See Fig. 13-27.

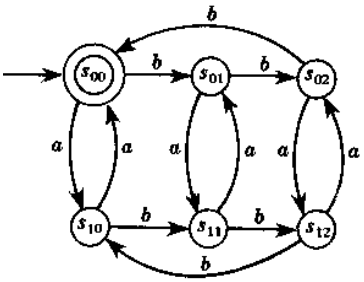


Fig. 13-27

13.63. $L(M)$ consists of all words w which contain $aabb$ as a subword.

13.64. (*a*) $A = (a, b)$, $S = \{s_0, s_1, s_2, s_3\}$, $Z = \{x, y, z\}$, and s_0 is the initial state.
(*b*) See Fig. 13-28.
(*c*) $v = y^2zyzxzxyz$.

13.65. (*a*) See Fig. 13-29. (*b*) $v = xy^2xz^3xyx$.

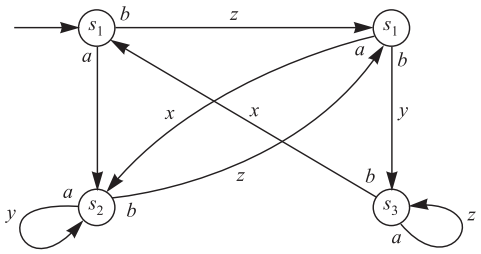


Fig. 13-28

F	a	b	c
s_0	s_1, x	s_2, z	s_1, x
s_1	s_1, y	s_2, z	s_0, z
s_0	s_1, z	s_2, x	s_0, x

Fig. 13-29

13.66. (*a*) $v = xyzxy^2z^2x^2z^2y^2$; (*b*) $v = zyxy^2zx^2zxy^2xy$.

13.67. (*a*) Type 2; (*b*) Type 0; (*c*) Type 3.

13.68. $S \to (a, b, aB, bA)$, $A \to (bA, ab, a, b)$, $B \to (b, bA)$.

13.69. $S \to (AAB,\ ABA,\ BAA)$, $A \to (a, BAAA,\ ABAA,\ AABA,\ AAAB)$,
$B \to (b,\ BBAA,\ BABA,\ aBAAB,\ ABAB,\ AABB)$.

13.70. $S \to (aSa, b)$.

13.72. $L = \{ab^{2n}c : n \geq 0\}$.

13.73. $L = \{a^n cb^n : n > 0\}$.

13.74. (*a*) $\langle S\rangle ::= a\langle A\rangle\langle B\rangle | \langle A\rangle\langle B\rangle$, $\langle A\rangle ::= a$, $\langle B\rangle ::= b$.
(*b*) Not defined for Type 0 language.
(*c*) $\langle S\rangle ::= a\langle B\rangle$, $\langle B\rangle ::= b\langle B\rangle | b\langle A\rangle$, $\langle A\rangle ::= a|b$.

13.75. (*a*) $\langle S\rangle ::= a|a\langle A\rangle\langle S\rangle$, $\langle A\rangle ::= b\langle S\rangle$; (*b*) See Fig. 13-30.

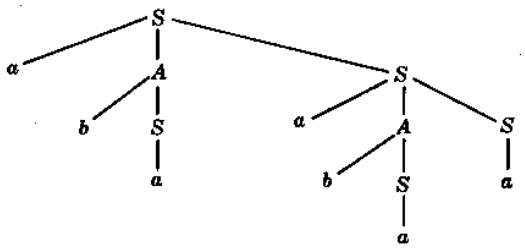


Fig. 13-30

13.76. (*a*) $w = aababa$; (*b*) $S \to aAB$, $A \to aB$, $B \to ba$.

13.77. (*a*) $\alpha = abs_2baa$; (*b*) $\alpha = aabs_3b$; (*c*) $\alpha = s_0aaabbb$; (*d*) $\alpha = s_0 1111B111$.

13.78. (*a*) $\beta = abbs_1a$; (*b*) $\beta = as_3baa$; (*c*) $\beta = abs_2ba$; (*d*) $\beta = as_3bba$; (*e*) α is not changed by q;
(*f*) $\beta = \alpha = abs_2aa$.

13.79. (*a*) $\beta = bs_1Bab$; (*b*) $\beta = s_2BaBab$; (*c*) $\beta = s_2bBab$; (*d*) $\beta = s_3BbBab$; (*e*) α is not changed by q;
(*f*) $\beta = \alpha = s_2aBab$.

13.80. $\alpha = s_0a$; $\beta = s_1b$, $q_1 = s_0abs_1N$; $q_2 = s_1Bas_0N$.

13.81. Yes.

13.82. No, since $\alpha \to \beta \to \alpha \to \beta \to \cdots$ never ends.

13.83. $q_1 = s_0BBs_NR$ (NO); $q_2 = s_0bbs_NR$ (NO);
$q_3 = s_0aas_1R$; $q_4 = s_1BBs_NR$ (NO);
$q_5 = s_1aas_NR$ (NO); $q_6 = s_1bbs_2R$; $q_7 = s_2bbs_2R$;
$q_8 = s_2aas_NR$ (NO); $q_9 = s_2BBs_YR$ (YES).

13.84. $q_1 = s_0BBs_NR$ (NO); $q_2 = s_0bbs_NR$ (NO);
$q_3 = s_0aas_1R$; $q_4 = s_1BBs_YR$ (accepts);
$q_5 = s_1bbs_NR$ (NO); $q_6 = s_1aas_2R$;
$q_7 = s_2BBs_YR$ (YES); $q_8 = s_2aas_NR$ (NO);
$q_9 = s_2bbs_NN$ (NO).

13.85. (*a*) $\langle 6\rangle = 1^7$; (*b*) $\langle m\rangle = 1^6B1B1^4B1^2$; (*c*) $\langle m\rangle = 1B1B1$; (*d*) not defined.

13.86. (*a*) $[E] = 7$; (*b*) $[E] = 2$; (*c*) $[E] = 14$.

13.87. Strategy: Erase first three 1s:
$q_1 = s_0 1Bs_1R$, $q_2 = s_1BBs_HN$ (halt), $q_3 = s_1 1Bs_2R$,
$q_4 = s_2BBs_HN$ (halt), $q_5 = s_2 1Bs_HN$

13.88. Strategy: Erase first 1 and then all 1s after B.
$q_1 = s_0 1Bs_1R$, $q_2 = s_1 11s_1R$, $q_3 = s_1BBs_2R$,
$q_4 = s_2 1Bs_3R$, $q_5 = s_3 1Bs_3R$, $q_6 = s_3BBs_HN$ (halt)

© The McGraw–Hill Companies, 2004

Chapter 14

Ordered Sets and Lattices

14.1 INTRODUCTION

Order and precedence relationships appear in many different places in mathematics and computer science. This chapter makes these notions precise. We also define a lattice, which is a special kind of an ordered set.

14.2 ORDERED SETS

Suppose R is a relation on a set S satisfying the following three properties:

$[\mathbf{O}_1]$ (Reflexive) For any $a \in S$, we have $a\,R\,a$.
$[\mathbf{O}_2]$ (Antisymmetric) If $a\,R\,b$ and $b\,R\,a$, then $a = b$.
$[\mathbf{O}_2]$ (Transitive) If $a\,R\,b$ and $b\,R\,c$, then $a\,R\,c$.

Then R is called a *partial order* or, simply an *order* relation, and R is said to define a *partial ordering* of S. The set S with the partial order is called a *partially ordered set* or, simply, an *ordered set* or *poset*. We write (S, R) when we want to specify the relation R.

The most familiar order relation, called the *usual order*, is the relation $\leq$ (read "less than or equal") on the positive integers $\mathbf{N}$ or, more generally, on any subset of the real numbers $\mathbf{R}$. For this reason, a partial order relation is usually denoted by $\preceq$; and

$$a \preceq b$$

is read "a precedes b". In this case we also write:

$a \prec b$ means $a \preceq b$ and $a \neq b$; read "a strictly precedes b".
$b \succeq a$ means $a \preceq b$; read "b succeeds a".
$b \succ a$ means $a \prec b$; read "b strictly succeeds a".
$\not\preceq$, $\not\prec$, $\not\succeq$, and $\not\succ$ are self-explanatory.

When there is no ambiguity, the symbols $\leq$, $<$, $>$, and $\geq$ are frequently used instead of $\preceq$, $\prec$, $\succ$, and $\succeq$, respectively.

EXAMPLE 14.1

(*a*) Let $\mathcal{S}$ be any collection of sets. The relation $\subseteq$ of set inclusion is a partial ordering of $\mathcal{S}$. Specifically, $A \subseteq A$ for any set A; if $A \subseteq B$ and $B \subseteq A$ then $A = B$; and if $A \subseteq B$ and $B \subseteq C$ then $A \subseteq C$.

(*b*) Consider the set $\mathbf{N}$ of positive integers. We say "a divides b", written $a|b$, if there exists an integer c such that $ac = b$. For example, $2\,|\,4$, $3\,|\,12$, $7\,|\,21$, and so on. This relation of divisibility is a partial ordering of $\mathbf{N}$.

(*c*) The relation "|" of divisibility is not an ordering of the set $\mathbf{Z}$ of integers. Specifically, the relation is not antisymmetric. For instance, $2\,|\,-2$ and $-2\,|\,2$, but $2 \neq -2$.

(*d*) Consider the set $\mathbf{Z}$ of integers. Define $a\,R\,b$ if there is a positive integer r such that $b = a^r$. For instance, $2\,R\,8$ since $8 = 2^3$. Then R is a partial ordering of $\mathbf{Z}$.

Dual Order

Let $\preceq$ be any partial ordering of a set S. The relation $\succeq$, that is, a succeeds b, is also a partial ordering of S; it is called the *dual order*. Observe that $a \preceq b$ if and only if $b \succeq a$; hence the dual order $\succeq$ is the inverse of the relation $\preceq$, that is, $\succeq = \preceq^{-1}$.

Ordered Subsets

Let A be a subset of an ordered set S, and suppose $a, b \in A$. Define $a \precsim b$ as elements of A whenever $a \precsim b$ as elements of S. This defines a partial ordering of A called the *induced order* on A. The subset A with the induced order is called an *ordered subset* of S. Unless otherwise stated or implied, any subset of an ordered set S will be treated as an ordered subset of S.

Quasi-order

Suppose $\prec$ is a relation on a set S satisfying the following two properties:

$[\mathbf{Q}_1]$ (Irreflexive) For any $a \in A$, we have $a \not\prec a$.
$[\mathbf{Q}_2]$ (Transitive) If $a \prec b$, and $b \prec c$, then $a \prec c$.

Then $\prec$ is called a *quasi-order* on S.

There is a close relationship between partial orders and quasi-orders. Specifically, if $\precsim$ is a partial order on a set S and we define $a \prec b$ to mean $a \precsim b$ but $a \neq b$, then $\prec$ is a quasi-order on S. Conversely, if $\prec$ is a quasi-order on a set S and we define $a \precsim b$ to mean $a \prec b$ or $a = b$, then $\precsim$ is a partial order on S. This allows us to switch back and forth between a partial order and its corresponding quasi-orders using whichever is more convenient.

Comparability, Linearly Ordered Sets

Suppose a and b are elements in a partially ordered set S. We say a and b are *comparable* if

$$a \precsim b \qquad \text{or} \qquad b \precsim a$$

that is, if one of them precedes the other. Thus a and b are *noncomparable*, written

$$a \parallel b$$

if neither $a \precsim b$ nor $b \precsim a$.

The word "partial" is used in defining a partially ordered set S since some of the elements of S need not be comparable. Suppose, on the other hand, that every pair of elements of S are comparable. Then S is said to be *totally ordered* or *linearly ordered*, and S is called a *chain*. Although an ordered set S may not be linearly ordered, it is still possible for a subset A of S to be linearly ordered. Clearly, every subset of a linearly ordered set S must also be linearly ordered.

EXAMPLE 14.2

(*a*) Consider the set $\mathbf{N}$ of positive integers ordered by divisibility. Then 21 and 7 are comparable since $7 \mid 21$. On the other hand, 3 and 5 are noncomparable since neither $3 \mid 5$ nor $5 \mid 3$. Thus $\mathbf{N}$ is not linearly ordered by divisibility. Observe that $A = \{2, 6, 12, 36\}$ is a linearly ordered subset of N since $2 \mid 6$, $6 \mid 12$ and $12 \mid 36$.

(*b*) The set $\mathbf{N}$ of positive integers with the usual order $\leq$ (less than or equal) is linearly ordered and hence every ordered subset of $\mathbf{N}$ is also linearly ordered.

(*c*) The power set $P(A)$ of a set A with two or more elements is not linearly ordered by set inclusion. For instance, suppose a and b belong to A. Then $\{a\}$ and $\{b\}$ are noncomparable. Observe that the empty set $\varnothing$, $\{a\}$, and A do form a linearly ordered subset of $P(A)$ since $\varnothing \subseteq \{a\} \subseteq A$. Similarly, $\varnothing$, $\{b\}$, and A form a linearly ordered subset of $P(A)$.

Product Sets and Order

There are a number of ways to define an order relation on the Cartesian product of given ordered sets. Two of these ways follow:

(*a*) ***Product Order***: Suppose S and T are ordered sets. Then the following, is an order relation on the product set $S \times T$, called the *product order*:

$$(a, b) \precsim (a', b') \qquad \text{if} \qquad a \leq a' \text{ and } b \leq b'$$

(*b*) ***Lexicographical Order***: Suppose S and T are linearly ordered sets. Then the following is an order relation on the product set $S \times T$, called the *lexicographical* or *dictionary order*:

$$(a, b) \prec (a', b') \qquad \text{if} \qquad a < b \qquad \text{or if} \qquad a = a' \text{ and } b < b'$$

This order can be extended to $S_1 \times S_2 \times \cdots \times S_n$ as follows:

$$(a_1, a_2, \cdots, a_n) \prec (a_1', a_2', \ldots, a_n') \qquad \text{if} \qquad a_i = a_i' \text{ for } i = 1, 2, \ldots, k-1 \text{ and } a_k < a_k'$$

Note that the lexicographical order is also linear.

Kleene Closure and Order

Let A be a (nonempty) linearly ordered alphabet. Recall that A^*, called the Kleene closure of A, consists of all words w on A, and $|\, w \,|$ denotes the length of w. Then the following are two order relations on A^*.

(*a*) ***Alphabetical (Lexicographical) Order***: The reader is no doubt familiar with the usual alphabetical ordering of A^*. That is:

(i) $\lambda < w$, where λ is the empty word and w is any nonempty word.

(ii) Suppose $u = au'$ and $v = bv'$ are distinct nonempty words where $a, b \in A$ and $u', v' \in A^*$. Then

$$u \prec v \qquad \text{if } a < b \qquad \text{or} \qquad \text{if } a = b \text{ but } u' \prec v'$$

(*b*) ***Short-lex Order***: Here A^* is ordered first by length, and then alphabetically. That is, for any distinct words u, v in A^*,

$$u \prec v \qquad \text{if } |\, u \,| < |\, v \,| \qquad \text{or if } |\, u \,| = |\, v \,| \text{ but } u \text{ precedes } v \text{ alphabetically}$$

For example, "to" precedes "and" since |to| = 2 but |and| = 3. However, "an" precedes "to" since they have the same length, but "an" precedes "to" alphabetically. This order is also called the *free semigroup order*.

14.3 HASSE DIAGRAMS OF PARTIALLY ORDERED SETS

Let S be a partially ordered set, and suppose a, b belong to S. We say that a is an *immediate predecessor* of b, or that b is an *immediate successor* of a, or that b is a *cover* of a, written

$$a \lessdot b$$

if $a < b$ but no element in S lies between a and b, that is, there exists no element c in S such that $a < c < b$.

Suppose S is a finite partially ordered set. Then the order on S is completely known once we know all pairs a, b in S such that $a \lessdot b$, that is, once we know the relation $\lessdot$ on S. This follows from the fact that $x < y$ if and only if $x \lessdot y$ or there exist elements $a_1, a_2, \ldots, a_m$ in S such that

$$x \lessdot a_1 \lessdot a_2 \lessdot \cdots \lessdot a_m \lessdot y$$

The *Hasse diagram* of a finite partially ordered set S is the directed graph whose vertices are the elements of S and there is a directed edge from a to b whenever $a \ll b$ in S. (Instead of drawing an arrow from a to b, we sometimes place b higher than a and draw a line between them. It is then understood that movement upwards indicates succession.) In the diagram thus created, there is a directed path from vertex x to vertex y if and only if $x < y$. Also, there can be no (directed) cycles in the diagram of S since the order relation is antisymmetric.

The Hasse diagram of a poset S is a picture of S; hence it is very useful in describing types of elements in S. Sometimes we define a partially ordered set by simply presenting its Hasse diagram. We note that the Hasse diagram of a poset S need not be connected.

Remark: The Hasse diagram of a finite poset S turns out to be a directed cycle-free graph (DAG) studied in Section 9.9. The investigation here is independent of the previous investigation. Here we mainly think of order in terms of "less than" or "greater than" rather than in terms of directed adjacency relations. Accordingly, there will be some overlap in the content.

EXAMPLE 14.3

(*a*) Let $A = \{1, 2, 3, 4, 6, 8, 9, 12, 18, 24\}$ be ordered by the relation "x divides y". The diagram of A is given in Fig. 14-1(*a*) (Unlike rooted trees, the direction of a line in the diagram of a poset is always upward.)

(*b*) Let $B = \{a, b, c, d, e\}$. The diagram in Fig. 14-1(*b*) defines a partial order on B in the natural way. That is, $d \leq b$, $d \leq a$, $e \leq c$ and so on.

(*c*) The diagram of a finite linearly ordered set, i.e., a finite chain, consists simply of one path. For example, Fig. 14-1(*c*) shows the diagram of a chain with five elements.

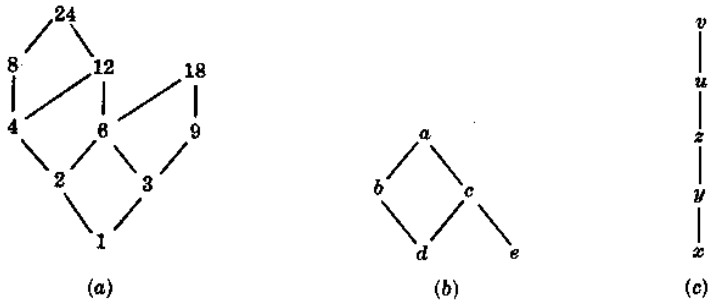


Fig. 14-1

EXAMPLE 14.4

A *partition* of a positive integer m is a set of positive integers whose sum is m. For instance, there are seven partitions of $m = 5$ as follows:

$$5, \quad 3-2, \quad 2-2-1, \quad 1-1-1-1-1, \quad 4-1, \quad 3-1-1, \quad 2-1-1-1$$

We order the partitions of an integer m as follows. A partition P_1 precedes a partition P_2 if the integers in P_1 can be added to obtain the integers in P_2 or, equivalently, if the integers in P_2 can be further subdivided to obtain the integers in P_1. For example,

$$2-2-1 \qquad \text{precedes} \qquad 3-2$$

since $2 + 1 = 3$. On the other hand, $3 - 1 - 1$ and $2 - 2 - 1$ are noncomparable.

Figure 14-2 gives the Hasse diagram of the partitions of $m = 5$.

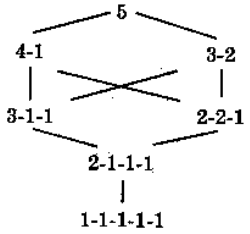


Fig. 14-2

Minimal and Maximal, and First and Last Elements

Let S be a partially ordered set. An element a in S is called a *minimal* element if no other element of S strictly precedes (is less than) a. Similarly, an element b in S is called a *maximal* element if no element of S strictly succeeds (is larger than) b. Geometrically speaking, a is a minimal element if no edge enters a (from below), and b is a maximal element if no edge leaves b (in the upward direction). We note that S can have more than one minimal and more than one maximal element.

If S is infinite, then S may have no minimal and no maximal element. For instance, the set $\mathbf{Z}$ of integers with the usual order $\leq$ has no minimal and no maximal element. On the other hand, if S is finite, then S must have at least one minimal element and at least one maximal element.

An element a is S is called a *first* element if

$$a \precsim x$$

for every element x in S, that is, if a precedes every other element in S. Similarly, an element b in S is called a *last* element if

$$y \precsim b$$

for every element y in S, that is, if b succeeds every other element in S. We note that S can have at most one first element, which must be a minimal element, and S can have at most one last element, which must be a maximal element. Generally speaking, S may have neither a first nor a last element, even when S is finite.

EXAMPLE 14.5

(*a*) Consider the three partially ordered sets in Example 14-3 whose Hasse diagrams appear in Fig. 14-1.

(i) A has two maximal elements 18 and 24 and neither is a last element. A has only one minimal element, 1, which is also a first element.

(ii) B has two minimal elements, d and e, and neither is a first element. B has only one maximal element, a, which is also a last element.

(iii) The chain has one minimal element, x, which is a first element, and one maximal element, v, which is a last element.

(*b*) Let A be any nonempty set and let $P(A)$ be the power set of A ordered by set inclusion. Then the empty set $\varnothing$ is a first element of $P(A)$ since, for any set X, we have $\varnothing \subseteq X$. Moreover, A is a last element of $P(A)$ since every element Y of $P(A)$ is, by definition, a subset of A, that is, $Y \subseteq A$.

14.4 CONSISTENT ENUMERATION

Suppose S is a finite partially ordered set. Frequently we want to assign positive integers to the elements of S in such a way that the order is preserved. That is, we seek a function $f: S \to \mathbf{N}$ so that if $a \prec b$ then $f(a) < f(b)$. Such a function is called a *consistent enumeration* of S. The fact that this can always be done is the content of the following theorem.

Theorem 14.1: There exists a consistent enumeration for any finite poset A.

We prove this theorem in Problem 14.15. In fact, we prove that if S has n elements then there exists a consistent enumeration $f: S \to \{1, 2, \ldots, n\}$.

We emphasize that such an enumeration need not be unique. For example, the following are two such enumerations for the poset in Fig. 14-1(b):

(i) $f(d) = 1,\ f(e) = 2,\ f(b) = 3,\ f(c) = 4,\ f(a) = 5.$

(ii) $g(e) = 1,\ g(d) = 2,\ g(c) = 3,\ g(b) = 4,\ g(a) = 5.$

However the chain in Fig. 14-1(c) admits only one consistent enumeration if we map the set into $\{1, 2, 3, 4, 5\}$. Specifically, we must assign:

$$h(x) = 1, \qquad h(y) = 2, \qquad h(z) = 3, \qquad h(u) = 4, \qquad h(v) = 5$$

14.5 SUPREMUM AND INFIMUM

Let A be a subset of a partially ordered set S. An element M in S is called an *upper bound* of A if M succeeds every element of A, i.e., if, for every x in A, we have

$$x \precsim M$$

If an upper bound of A precedes every other upper bound of A, then it is called the *supremum* of A and is denoted by

$$\sup(A)$$

We also write $\sup(a_1, \ldots, a_n)$ instead of $\sup(A)$ if A consists of the elements $a_1, \ldots, a_n$. We emphasize that there can be at most one $\sup(A)$; however, $\sup(A)$ may not exist.

Analogously, an element m in a poset S is called a *lower bound* of a subset A of S if m precedes every element of A, i.e., if, for every y in A, we have

$$m \precsim y$$

If a lower bound of A succeeds every other lower bound of A, then it is called the *infimum* of A and is denoted by

$$\inf(A), \qquad \text{or} \qquad \inf(a_1, \ldots, a_n)$$

if A consists of the elements $a_1, \ldots, a_n$. There can be at most one $\inf(A)$ although $\inf(A)$ may not exist.

Some texts use the term *least upper bound* instead of supremum and then write $\text{lub}(A)$ instead of $\sup(A)$, and use the term *greatest lower bound* instead of infimum and write $\text{glb}(A)$ instead of $\inf(A)$.

If A has an upper bound we say A is *bounded above*, and if A has a lower bound we say A is *bounded below*. In particular, A is *bounded* if A has an upper and lower bound.

EXAMPLE 14.6

(a) Let $S = \{a, b, c, d, e, f\}$ be ordered as pictured in Fig. 14-3(a), and let $A = \{b, c, d\}$. The upper bounds of A are e and f since only e and f succeed every element in A. The lower bounds of A are a and b since only a and b precede every element of A. Note that e and f are noncomparable; hence $\sup(A)$ does not exist. However, b also succeeds a, hence $\inf(A) = b$.

(b) Let $S = \{1, 2, 3, \ldots, 8\}$ be ordered as pictured in Fig. 14-3(b), and let $A = \{4, 5, 7\}$. The upper bounds of A are 1, 2, and 3, and the only lower bound is 8. Note that 7 is not a lower bound since 7 does not precede 4. Here $\sup(A) = 3$ since 3 precedes the other upper bounds 1 and 2. Note that $\inf(A) = 8$ since 8 is the only lower bound.

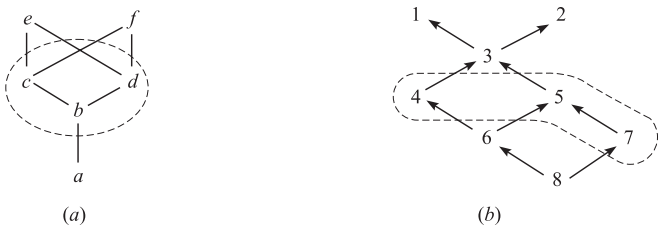


Fig. 14-3

Generally speaking, $\sup(a, b)$ and $\inf(a, b)$ need not exist for every pair of elements a and b in a poset S. We now give two examples of partially ordered sets where $\sup(a, b)$ and $\inf(a, b)$ do exist for every a, b in the set.

EXAMPLE 14.7

(*a*) Let the set **N** of positive integers be ordered by divisibility. The *greatest common divisor* of a and b in **N**, denoted by

$$\gcd(a, b)$$

is the largest integer which divides a and b. The *least common multiple* of a and b, denoted by

$$\text{lcm}(a, b)$$

is the smallest integer divisible by both a and b.

An important theorem in number theory says that every common divisor of a and b divides $\gcd(a, b)$. One can also prove that $\text{lcm}(a, b)$ divides every multiple of a and b. Thus

$$\gcd(a, b) = \inf(a, b) \qquad \text{and} \qquad \text{lcm}(a, b) = \sup(a, b)$$

In other words, $\inf(a, b)$ and $\sup(a, b)$ do exist for any pair of elements of **N** ordered by divisibility.

(*b*) For any positive integer m, we will let $\mathbf{D}_m$ denote the set of divisors of m ordered by divisibility. The Hasse diagram of

$$\mathbf{D}_{36} = \{1, 2, 3, 4, 6, 9, 12, 18, 36\}$$

appears in Fig. 14-4. Again, $\inf(a, b) = \gcd(a, b)$ and $\sup(a, b) = \text{lcm}(a, b)$ exist for any pair a, b in $\mathbf{D}_m$.

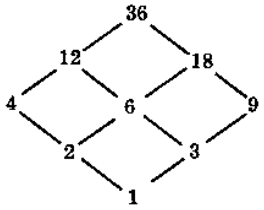


Fig. 14-4

14.6 ISOMORPHIC (SIMILAR) ORDERED SETS

Suppose X and Y are partially ordered sets. A one-to-one (injective) function $f: X \to Y$ is called a *similarity mapping* from X into Y if f preserves the order relation, that is, if the following two conditions hold for any pair a and a' in X:

(1) If $a \precsim a'$ then $f(a) \precsim f(a')$.
(2) If $a \| a'$ (noncomparable), then $f(a) \| f(b)$.

Accordingly, if A and B are linearly ordered, then only (1) is needed for f to be a similarity mapping.

Two ordered sets X and Y are said to be *isomorphic* or *similar*, written

$$X \simeq Y$$

if there exists a one-to-one correspondence (bijective mapping) $f: X \to Y$ which preserves the order relations, i.e., which is a similarity mapping.

EXAMPLE 14.8 Suppose $X = \{1, 2, 6, 8, 12\}$ is ordered by divisibility and suppose $Y = \{a, b, c, d, e\}$ is isomorphic to X; say, the following function f is a similarity mapping from X onto Y:

$$f = \{(1, e),\ (2, d),\ (6, b),\ (8, c),\ (12, a)\}$$

Draw the Hasse diagram of Y.

The similarity mapping preserves the order of the initial set X and is one-to-one and onto. Thus the mapping can be viewed simply as a relabeling of the vertices in the Hasse diagram of the initial set X. The Hasse diagrams for both X and Y appear in Fig. 14-5.

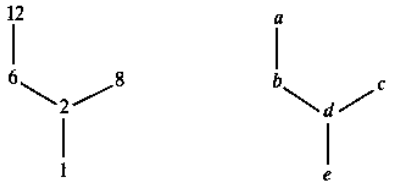


Fig. 14-5

14.7 WELL-ORDERED SETS

We begin with a definition.

Definition: An ordered set S is said to be *well-ordered* if every subset of S has a first element.

The classical example of a well-ordered set is the set $\mathbf{N}$ of positive integers with the usual order $\leq$. The following facts follow from the definition.

(1) A well-ordered set is linearly ordered. For if $a, b, \in S$, then $\{a, b\}$ has a first element; hence a and b are comparable.
(2) Every subset of a well-ordered set is well-ordered.
(3) If X is well-ordered and Y is isomorphic to X, then Y is well-ordered.
(4) All finite linearly ordered sets with the same number n of elements are well-ordered and are all isomorphic to each other. In fact, they are all isomorphic to $\{1, 2, \ldots, n\}$ with the usual order $\leq$.
(5) Every element $a \in S$, other than a last element, has an immediate successor. For, let $M(a)$ denote the set of elements which strictly succeed a. Then the first element of $M(a)$ is the immediate successor of a.

EXAMPLE 14.9

(*a*) The set **Z** of integers with the usual order $\leq$ is linearly ordered and every element has an immediate successor and an immediate predecessor, but **Z** is not well-ordered. For example, **Z** itself has no first element. However, any subset of **Z** which is bounded from below is well-ordered.

(*b*) The set **Q** of rational numbers with the usual order $\leq$ is linearly ordered, but no element in **Q** has an immediate successor or an immediate predecessor. For if $a, b \in Q$, say $a < b$, then $(a+b)/2 \in \mathbf{Q}$ and

$$a < \frac{a+b}{2} < b$$

(*c*) Consider the disjoint well-ordered sets

$$A = \{1, 3, 5, \ldots, \} \qquad \text{and} \qquad B = \{2, 4, 6, \ldots\}$$

Then the following ordered set

$$S = \{A; B\} = \{1, 3, 5, \ldots; 2, 4, 6, \ldots\}$$

is well-ordered. Note that, besides the first element 1, the element 2 does not have an immediate predecessor.

Notation: Here and subsequently, if $A, B, \ldots$ are disjoint ordered sets, then $\{A; B; \ldots\}$ means the set $A \cup B \cup \ldots$ ordered positionwise from left to right; that is, the elements in the same set keep their order, and any element in a set on the left precedes any element in a set on its right. Thus every element in A precedes every element in B, and so on.

Transfinite Induction

First we restate the principle of mathematical induction. (See Section 1.10 and 11.3.)

Principle of Mathematical Induction: Let A be a subset of the set **N** of positive integers with the following two properties:

(i) $1 \in A$.

(ii) If $n \in A$, then $n + 1 \in A$.

Then $A = \mathbf{N}$.

The above principle is one of Peano's axioms for the natural numbers (positive integers) **N**. There is another form which is sometimes more convenient to use. Namely:

Principle of Mathematical Induction (Second Form): Let A be a subset of **N** with the following two properties:

(i) $1 \in A$.

(ii) If k belongs to A for $1 \leq k < n$, then $n \in A$.

Then $A = \mathbf{N}$.

The second form of induction is equivalent to the fact that **N** is well-ordered (Theorem 11.6). In fact, there is a somewhat similar statement which is true for every well-ordered set.

Principle of Transfinite Induction: Let A be a subset of a well-ordered set S with the following two properties:

(i) $a_0 \in A$.

(ii) If $s(a) \subseteq A$, then $a \in A$.

Then $A = S$.

Here a_0 is the first element of S, and $s(a)$, called the *initial segment* of a, is defined to be the set of all elements of S which strictly precede a.

Axiom of Choice, Well-Ordering Theorem

Let $\{A_i : i \in I\}$ be a collection of nonempty disjoint sets. We assume every $A_i \subseteq X$. A function $f : \{A_i\} \to X$ is called a *choice function* if $f(A_i) = a_i \in A_i$. In other words, f "chooses" a point $a_i \in A_i$ for each set A_i.

The axiom of choice lies at the foundations of mathematics and, in particular, the theory of sets. This "innocent looking" axiom, which follows, has as a consequence some of the most powerful and important results in mathematics.

Axiom of Choice: There exists a choice function for any nonempty collection of nonempty disjoint sets.

One of the consequences of the axiom of choice is the following theorem, which is attributed to Zermelo.

Well-Ordering Theorem: Every set S can be well-ordered.

The proof of this theorem lies beyond the scope of this text. Moreover, since all of our structures are finite or countable, we will not need to use this theorem. Ordinary mathematical induction suffices.

14.8 LATTICES

Let L be a nonempty set closed under two binary operations called *meet* and *join*, denoted respectively by $\wedge$ and $\vee$. Then L is called a *lattice* if the following axioms hold where a, b, c are elements in L:

$[\mathbf{L}_1]$ Commutative law:
$(1a)$ $a \wedge b = b \wedge a$ $\qquad$ $(1b)$ $a \vee b = b \vee a$

$[\mathbf{L}_2]$ Associative law:
$(2a)$ $(a \wedge b) \wedge c = a \wedge (b \wedge c)$ $\qquad$ $(2b)$ $(a \vee b) \vee c = a \vee (b \vee c)$

$[\mathbf{L}_3]$ Absorption law:
$(3a)$ $a \wedge (a \vee b) = a$ $\qquad$ $(3b)$ $a \vee (a \wedge b) = a$

We will sometimes denote the lattice by $(L, \wedge, \vee)$ when we want to show which operations are involved.

Duality and the Idempotent Law

The *dual* of any statement in a lattice $(L, \wedge, \vee)$ is defined to be the statement that is obtained by interchanging $\wedge$ and $\vee$. For example, the dual of

$$a \wedge (b \vee a) = a \vee a \qquad \text{is} \qquad a \vee (b \wedge a) = a \wedge a$$

Notice that the dual of each axiom of a lattice is also an axiom. Accordingly, the principle of duality holds; that is:

Theorem 14.2 (Principle of Duality): The dual of any theorem in a lattice is also a theorem.

This follows from the fact that the dual theorem can be proven by using the dual of each step of the proof of the original theorem.

An important property of lattices follows directly from the absorption laws.

Theorem 14.3 (Idempotent Law): (i) $a \wedge a = a$, (ii) $a \vee a = a$.

The proof of (i) requires only two lines:

$$\begin{aligned} a \wedge a &= a \wedge (a \vee (a \wedge b)) && (\text{using } (3b)) \\ &= a && (\text{using } (3a)) \end{aligned}$$

The proof of (ii) follows from the above principle of duality (or can be proved in a similar manner).

Lattices and Order

Given a lattice L, we can define a partial order on L as follows:

$$a \precsim b \qquad \text{if} \qquad a \wedge b = a$$

Analogously, we could define

$$a \precsim b \qquad \text{if} \qquad a \vee b = b$$

We state these results in a theorem.

Theorem 14.4: Let L be a lattice. Then:
(i) $a \wedge b = a$ if and only if $a \vee b = b$.
(ii) The relation $a \precsim b$ (defined by $a \wedge b = a$ or $a \vee b = b$) is a partial order on L.

Now that we have a partial order on any lattice L, we can picture L by a diagram as was done for partially ordered sets in general.

EXAMPLE 14.10 Let C be a collection of sets closed under intersection and union. Then $(C, \cap, \cup)$ is a lattice. In this lattice, the partial order relation is the same as the set inclusion relation. Figure 14-6 shows the diagram of the lattice L of all subsets of $\{a, b, c\}$.

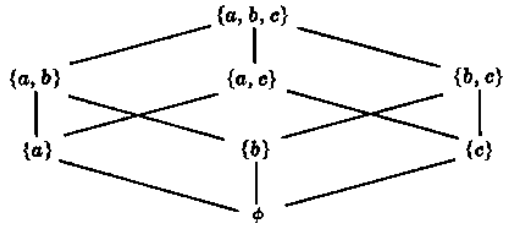


Fig. 14-6

We have shown how to define a partial order on a lattice L. The next theorem tells us when we can define a lattice on a partially ordered set P such that the lattice will give back the original order on P.

Theorem 14.5: Let P be a poset such that the $\inf(a, b)$ and $\sup(a, b)$ exist for any a, b in P. Letting

$$a \wedge b = \inf(a, b) \qquad \text{and} \qquad a \vee b = \sup(a, b)$$

we have that $(P, \wedge, \vee)$ is a lattice. Furthermore, the partial order on P induced by the lattice is the same as the original partial order on P.

The converse of the above theorem is also true. That is, let L be a lattice and let $\precsim$ be the induced partial order on L. Then $\inf(a, b)$ and $\sup(a, b)$ exist for any pair a, b in L and the lattice obtained from the poset $(L, \precsim)$ is the original lattice. Accordingly, we have the following:

Alternate Definition: A lattice is a partially ordered set in which

$$a \wedge b = \inf(a, b) \qquad \text{and} \qquad a \vee b = \sup(a, b)$$

exist for any pair of elements a and b.

We note first that any linearly ordered set is a lattice since $\inf(a, b) = a$ and $\sup(a, b) = b$ whenever $a \precsim b$. By Example 14.7, the positive integers $\mathbf{N}$ and the set $\mathbf{D}_m$ of divisors of m are lattices under the relation of divisibility.

Sublattices, Isomorphic Lattices

Suppose M is a nonempty subset of a lattice L. We say M is a *sublattice* of L if M itself is a lattice (with respect to the operations of L). We note that M is a sublattice of L if and only if M is closed under the operations of $\wedge$ and $\vee$ of L. For example, the set $\mathbf{D}_m$ of divisors of m is a sublattice of the positive integers $\mathbf{N}$ under divisibility.

Two lattices L and L' are said to be *isomorphic* if there is a one-to-one correspondence $f: L \to L'$ such that

$$f(a \wedge b) = f(a) \wedge f(b) \qquad \text{and} \qquad f(a \vee b) = f(a) \vee f(b)$$

for any elements a, b in L.

14.9 BOUNDED LATTICES

A lattice L is said to have a *lower bound* 0 if for any element x in L we have $0 \precsim x$. Analogously, L is said to have an *upper bound* I if for any x in L we have $x \precsim I$. We say L is *bounded* if L has both a lower bound 0 and an upper bound I. In such a lattice we have the identities

$$a \vee I = I, \qquad a \wedge I = a, \qquad a \vee 0 = a, \qquad a \wedge 0 = 0$$

for any element a in L.

The nonnegative integers with the usual ordering,

$$0 < 1 < 2 < 3 < 4 < \dots$$

have 0 as a lower bound but have no upper bound. On the other hand, the lattice $P(U)$ of all subsets of any universal set U is a bounded lattice with U as an upper bound and the empty set $\varnothing$ as a lower bound.

Suppose $L = \{a_1, a_2, \dots, a_n\}$ is a finite lattice. Then

$$a_1 \vee a_2 \vee \cdots \vee a_n \qquad \text{and} \qquad a_1 \wedge a_2 \wedge \cdots \wedge a_n$$

are upper and lower bounds for L, respectively. Thus we have

Theorem 14.6: Every finite lattice L is bounded.

14.10 DISTRIBUTIVE LATTICES

A lattice L is said to be *distributive* if for any elements a, b, c in L we have the following:

[$\mathbf{L}_4$] Distributive law:

$$(4a)\ a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c) \qquad (4b)\ a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$$

Otherwise, L is said to be *nondistributive*. We note that by the principle of duality the condition $(4a)$ holds if and only if $(4b)$ holds.

Figure 14-7(a) is a nondistributive lattice since

$$a \vee (b \wedge c) = a \vee 0 = a \qquad \text{but} \qquad (a \vee b) \wedge (a \vee c) = I \wedge c = c$$

Figure 14-7(b) is also a nondistributive lattice. In fact, we have the following characterization of such lattices.

Theorem 14.7: A lattice L is nondistributive if and only if it contains a sublattice isomorphic to Fig. 14-7(a) or (b).

The proof of this theorem lies beyond the scope of this text.

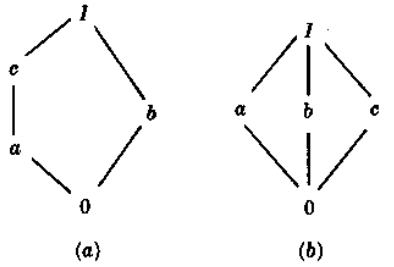


Fig. 14-7

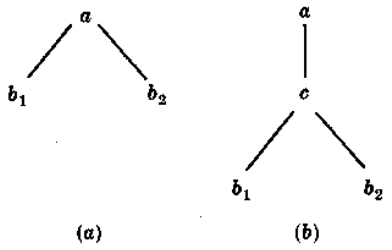


Fig. 14-8

Join Irreducible Elements, Atoms

Let L be a lattice with a lower bound 0. An element a in L is said to be *join irreducible* if $a = x \vee y$ implies $a = x$ or $a = y$. (Prime numbers under multiplication have this property, i.e., if $p = ab$ then $p = a$ or $p = b$ where p is prime.) Clearly 0 is join irreducible. If a has at least two immediate predecessors, say, b_1 and b_2 as in Fig. 14-8(a), then $a = b_1 \vee b_2$, and so a is not join irreducible. On the other hand, if a has a unique immediate predecessor c, then $a \neq \sup(b_1, b_2) = b_1 \vee b_2$ for any other elements b_1 and b_2 because c would lie between the b's and a as in Fig. 14-8(b). In other words, $a \neq 0$, is join irreducible if and only if a has a unique immediate predecessor. Those elements which immediately succeed 0, called *atoms*, are join irreducible. However, lattices can have other join irreducible elements. For example, the element c in Fig. 14-7(a) is not an atom but is join irreducible since a is its only immediate predecessor.

If an element a in a finite lattice L is not join irreducible, then we can write $a = b_1 \vee b_2$. Then we can write b_1 and b_2 as the join of other elements if they are not join irreducible; and so on. Since L is finite we finally have

$$a = d_1 \vee d_2 \vee \cdots \vee d_n$$

where the d's are join irreducible. If d_i precedes d_j then $d_i \vee d_j = d_j$; so we can delete the d_i from the expression. In other words, we can assume that the d's are *irredundant*, i.e., no d precedes any other d. We emphasize that such an expression need not be unique, e.g., $I = a \vee b$ and $I = b \vee c$ in both lattices in Fig. 14-7. We now state the main theorem of this section (proved in Problem 14.38).

Theorem 14.8: Let L be a finite distributive lattice. Then every a in L can be written uniquely (except for order) as the join of irredundant join irreducible elements.

Actually this theorem can be generalized to lattices with *finite length*, i.e., where all linearly ordered subsets are finite. (Problem 14.33 gives an infinite lattice with finite length.)

14.11 COMPLEMENTS, COMPLEMENTED LATTICES

Let L be a bounded lattice with lower bound 0 and upper bound I. Let a be an element of L. An element x in L is called a *complement* of a if

$$a \vee x = I \qquad \text{and} \qquad a \wedge x = 0$$

Complements need not exist and need not be unique. For example, the elements a and c are both complements of b in Fig. 14-7(a). Also, the elements y, z, and u in the chain in Fig. 14-1 have no complements. We have the following result.

Theorem 14.9: Let L be a bounded distributive lattice. Then complements are unique if they exist.

Proof: Suppose x and y are complements of any element a in L. Then

$$a \vee x = I, \qquad a \vee y = I, \qquad a \wedge x = 0, \qquad a \wedge y = 0$$

Using distributivity,

$$x = x \vee 0 = x \vee (a \wedge y) = (x \vee a) \wedge (x \vee y) = I \wedge (x \vee y) = x \vee y$$

Similarly,

$$y = y \vee 0 = y \vee (a \wedge x) = (y \vee a) \wedge (y \vee x) = I \wedge (y \vee x) = y \vee x$$

Thus

$$x = x \vee y = y \vee x = y$$

and the theorem is proved.

Complemented Lattices

A lattice L is said to be *complemented* if L is bounded and every element in L has a complement. Figure 14-7(b) shows a complemented lattice where complements are not unique. On the other hand, the lattice $P(U)$ of all subsets of a universal set U is complemented, and each subset A of U has the unique complement $A^c = U \backslash A$.

Theorem 14.10: Let L be a complemented lattice with unique complements. Then the join irreducible elements of L, other than 0, are its atoms.

Combining this theorem and Theorems 14.8 and 14.9, we get an important result.

Theorem 14.11: Let L be a finite complemented distributive lattice. Then every element a in L is the join of a unique set of atoms.

Remark: Some texts define a lattice L to be complemented if each a in L has a unique complement. Theorem 14.10 is then stated differently.

Solved Problems

ORDERED SETS AND SUBSETS

14.1. Suppose the set $\mathbf{N} = \{1, 2, 3, \ldots\}$ of positive integers is ordered by divisibility. Insert the correct symbol, $\prec$, $\succ$, or $\|$ (not comparable), between each pair of numbers:

(a) 2 ____ 8; (b) 18 ____ 24; (c) 9 ____ 3; (d) 5 ____ 15.

(a) Since 2 divides 8, 2 precedes 8, i.e., $2 \prec 8$.

(b) 18 does not divide 24, and 24 does not divide 18; hence $18 \| 24$.

(c) Since 9 is divisible by 3, $9 \succ 3$.

(d) Since 5 divides 15, $5 \prec 15$.

14.2. Let $\mathbf{N} = \{1, 2, 3, \ldots\}$ be ordered by divisibility. State whether each of the following subsets of $\mathbf{N}$ are linearly (totally) ordered.

(*a*) $\{24, 2, 6\}$ (*c*) $\mathbf{N} = \{1, 2, 3 \ldots\}$ (*e*) $\{7\}$.
(*b*) $\{3, 15, 5\}$ (*d*) $\{2, 8, 32, 4\}$ (*f*) $\{15, 5, 30\}$

(*a*) Since 2 divides 6 which divides 24, the set is linearly ordered.
(*b*) Since 3 and 5 are not comparable, the set is not linearly ordered.
(*c*) Since 2 and 3 are not comparable, the set is not linearly ordered.
(*d*) This set is linearly ordered since $2 \prec 4 \prec 8 \prec 32$.
(*e*) Any set consisting of one element is linearly ordered.
(*f*) Since 5 divides 15 which divides 30, the set is linearly ordered.

14.3. Let $A = \{1, 2, 3, 4, 5\}$ be ordered by the Hasse diagram in Fig. 14-9. Insert the correct symbol, $\prec$, $\succ$, or $\|$ (not comparable), between each pair of elements:

(*a*) 1 ____ 5; (*b*) 2 ____ 3; (*c*) 4 ____ 1; (*d*) 3 ____ 4.

(*a*) Since there is a "path" (edges slanting upward) from 5 to 3 to 1, 5 precedes 1; hence $1 \succ 5$.
(*b*) There is no path from 2 to 3, or vice versa; hence $2 \| 3$.
(*c*) There is a path from 4 to 2 to 1; hence $4 \prec 1$.
(*d*) Neither $3 \prec 4$ nor $4 \succ 3$; hence $3 \| 4$.

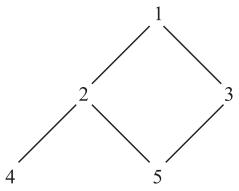


Fig. 14-9

14.4. Consider the ordered set A in Fig. 14-9.

(*a*) Find all minimal and maximal elements of A.
(*b*) Does A have a first element or a last element?

(*a*) No element strictly precedes 4 or 5, so 4 and 5 are minimal elements of A. No element strictly succeeds 1, so 1 is a maximal element of A.
(*b*) A has no first element. Although 4 and 5 are minimal elements of A, neither precedes the other. However, 1 is a last element of A since 1 succeeds every element of A.

14.5. Consider the ordered set A in Fig. 14-9. Let $L(A)$ denote the collection of all linearly ordered subsets of A with 2 or more elements. Let $L(A)$ be ordered by set inclusion. Draw the Hasse diagram of $L(A)$.

The elements of $L(A)$ are as follows:

$$\{1,2,4\}, \quad \{1,2,5\}, \quad \{1,3,5\} \quad \{1,2\}, \quad \{1,4\}, \quad \{1,3\}, \quad \{1,5\}, \quad \{2,4\}, \quad \{2,5\}, \quad \{3,5\}$$

(Note $\{2,5\}$ and $\{3,4\}$ are not linearly ordered.) The diagram of $L(A)$ appears in Fig. 14-10.

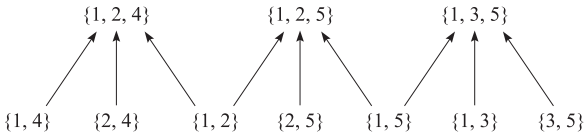


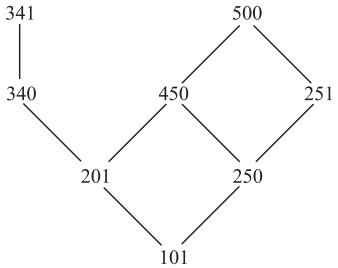
Fig. 14-10

14.6. Prerequisites in college is a familiar partial ordering of available classes. We say $A \ll B$ if course A is a prerequisite for course B. Consider the mathematics courses and their prerequisites given in Fig. 14-11(*a*). Draw the Hasse diagram for the partial ordering of these classes.

Math 101 must be on the bottom of the diagram since it is the only course with no prerequisites. Since Math 201 and Math 250 only require Math 101, we have Math 101 $\ll$ Math 201 and Math 101 $\ll$ Math 250; hence draw a line slanting upward from Math 101 to Math 201 and one from Math 101 to Math 250. Continuing this process, we obtain the Hasse diagram in Fig. 14-11(*b*).

Class	Prerequisites
Math 101	None
Math 201	Math 101
Math 250	Math 101
Math 251	Math 250
Math 340	Math 201
Math 341	Math 340
Math 450	Math 201, Math 250
Math 500	Math 450, Math 251

(*a*)



(*b*)

Fig. 14-11

14.7. Consider the ordered set C of mathematics classes in Fig. 14-11.

(*a*) Find all minimal and maximal elements of C.

(*b*) Does C have a first element or a last element?

(*a*) No element strictly precedes Math 101 so Math 101 is a minimal element of C. No element strictly succeeds Math 341 or Math 500, so each is a maximal element of C.

(*b*) Math 101 is a first element of C since it precedes every other element of C. However, C has no last element. Although Math 341 and Math 500 are maximal elements, neither is a last element since neither precedes the other.

14.8. Consider the set $\{\mathbf{N} = \{1, 2, 3, \ldots\}$ of positive integers. Every number in $\mathbf{N}$ can be written uniquely as a product of a nonnegative power of 2 times an odd number. Suppose a and a' are positive integers such that

$$a = 2^r(2s + 1) \qquad \text{and } a' \qquad = 2^{r'}(2s' + 1)$$

where r and s are nonnegative integers. We define:

$$a \prec a' \qquad \text{if } r < r' \qquad \text{or if} \qquad r = r' \text{ but } s < s'$$

Insert the correct symbol, $\prec$ or $\succ$, between each of the following pairs of numbers:

(*a*) 5 ____ 14; (*b*) 6 ____ 9; (*c*) 3 ____ 20; (*d*) 14 ____ 21.

The elements of $\mathbf{N}$ can be listed as in Fig. 14-12. The first row consists of the odd numbers, and the second row of 2 times the odd numbers, the third row of $2^2 = 4$ times the odd numbers, and so on. Then $a \prec a'$ if a is in a higher row than a', or if a and a' are in the same row but a comes before a' in the row. Thus:

(*a*) $5 \prec 14$; (*b*) $6 \succ 9$; (*c*) $3 \succ 20$; (*d*) $14 \succ 21$.

r \ s	0	1	2	3	4	5	6	7	
0	1	3	5	7	9	11	13	15	...
1	2	6	10	14	18	22	26	30	...
2	4	12	20	28	36	44	52	60	...
	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	

Fig. 14-12

PRODUCT SETS AND ORDER

14.9. Suppose $\mathbf{N}^2 = \mathbf{N} \times \mathbf{N}$ is given the product order (Section 14.2) where $\mathbf{N}$ has the usual order $\leq$. Insert the correct symbol, $\prec$, $\succ$, or $\|$ (not comparable), between each of the following pairs of elements of $\mathbf{N} \times \mathbf{N}$:

(*a*) $(5,7)\_\_(7,1)$ (*c*) $(5,5)\_\_(4,8)$ (*e*) $(7,9)\_\_(4,1)$

(*b*) $(4,6)\_\_(4,2)$ (*d*) $(1,3)\_\_(1,7)$ (*f*) $(7,9)\_\_(8,2)$

Here $(a,b) \precsim (a',b')$ provided $a \leq a'$ and $b \leq b'$. Hence $(a,b) \prec (a',b')$ if $a < a'$ and $b \leq b'$ or if $a \leq a'$ and $b < b'$. Thus:

(*a*) $\|$ since $5 < 7$ but $7 > 1$. (*c*) $\|$ since $5 > 4$ and $5 < 8$. (*e*) $\succ$ since $7 > 4$ and $9 > 1$.

(*b*) $\succ$ since $4 \geq 4$ and $6 > 2$. (*d*) $\prec$ since $1 \leq 1$ and $3 < 7$. (*f*) $\|$ since $7 < 8$ and $9 > 2$.

14.10. Repeat Problem 14.9 using the lexicographical ordering of $\mathbf{N}^2 = \mathbf{N} \times \mathbf{N}$.

Here $(a,b) \prec (a',b')$ if $a < a'$ or if $a = a'$ but $b < b'$. Thus:

(*a*) $\prec$ since $5 < 7$. (*c*) $\succ$ since $5 > 4$. (*e*) $\succ$ since $7 > 4$.

(*b*) $\succ$ since $4 = 4$ and $6 > 2$. (*d*) $\prec$ since $1 = 1$ but $3 < 7$. (*f*) $\prec$ since $7 < 8$.

14.11. Suppose the English alphabet $\mathbf{A} = \{a, b, c, \cdots, y, z\}$ is given the *usual (alphabetical) order*, and suppose $\mathbf{A}^2 = \mathbf{A} \times \mathbf{A}$ is given the product order. Insert the correct symbol, $\prec$, $\succ$, or $\|$ (not comparable), between each of the following two-letter words (viewed as elements of $\mathbf{A} \times \mathbf{A}$):

(*a*) *cx*__*at* (*c*) *cx*__*cz* (*e*) *cx*__*dx*

(*b*) *cx*__*by* (*d*) *cx*__*rs* (*f*) *cx*__*cs*

(*a*) $\succ$ since $c > a$ and $x > t$. (*c*) $\prec$ since $c \leq c$ and $x < z$. (*e*) $\prec$ since $c < d$ and $x \leq x$.

(*b*) $\|$ since $c > b$ but $x < y$. (*d*) $\|$ since $c < r$ but $x > s$. (*f*) $\succ$ since $c \geq c$ and $x > s$.

14.12. Repeat Problem 14.11 using the lexicographical (dictionary) ordering of $\mathbf{A}^2 = \mathbf{A} \times \mathbf{A}$.

(*a*) $\succ$ since $c > a$. (*c*) $\prec$ since $c = c$ and $x < z$. (*e*) $\prec$ since $c < d$.
(*b*) $\succ$ since $c > b$. (*d*) $\prec$ since $c < r$. (*f*) $\succ$ since $c = c$ and $x > s$.

14.13. Consider the English alphabet $\mathbf{A} = \{a, b, c, \ldots, y, z\}$ with the *usual (alphabetical) order*. Suppose A^*, consisting of all words in A, is given the lexico-length (free semigroup) order. Sort the following elements of $\mathbf{A}^*$:

went, forget, to, medicine, me, toast, melt, for, we, arm

First order the elements by length and then order them lexicographically (alphabetically):

me, to, we, arm, for, melt, went, toast, forget, medicine

14.14. Repeat Problem 14.13 using the usual (alphabetical) ordering of $\mathbf{A}^*$.

The usual ordering yields:

arm, for, forget, me, medicine, melt, to, toast, we, went

CONSISTENT ENUMERATIONS

14.15. Let $S = \{a, b, c, d, e\}$ be ordered as in Fig. 14.13. Find all possible consistent enumerations $f: S \to \{1, 2, 3, 4, 5\}$.

Since a is the only minimal element $f(a) = 1$, and since e is the only maximal element $f(e) = 5$. Also $f(b) = 2$ since b is the only successor of a. The choices for c and d are $f(c) = 3$ and $f(d) = 4$ or vice versa. Thus there are two possible enumerations, which follow:

(i) $f(a) = 1$, $f(b) = 2$, $f(c) = 3$, $f(d) = 4$, $f(e) = 5$
(ii) $f(a) = 1$, $f(b) = 2$, $f(c) = 4$, $f(d) = 3$, $f(e) = 5$

We emphasize that we usually cannot recreate the original partial order from a given consistent enumeration.

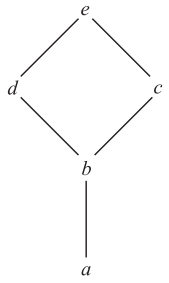


Fig. 14-13

14.16. Prove Theorem 14.1: Suppose S is a finite poset with n elements. Then there exists a consistent enumeration $f: S \to \{1, 2, \ldots, n\}$.

The proof is by induction on the number n of elements in S. Suppose $n = 1$, say $S = \{s\}$. Then $f(s) = 1$ is a consistent enumeration of S. Now suppose $n > 1$ and the theorem holds for posets with fewer than n elements. Let a in S be a minimal element. [Such an element a exists since S is finite.] Let $T = S \backslash \{a\}$. Then T

is a finite poset with $n-1$ elements and hence, by induction, T admits a consistent enumeration; say $g: T \to \{1, 2, \ldots, n-1\}$. Define $f: S \to \{1, 2, \ldots, n\}$ by

$$f(x) = \begin{cases} 1, & \text{if } x = a \\ g(x) + 1, & \text{if } x \neq a \end{cases}$$

Then f is the required consistent enumeration.

14.17. Suppose a student wants to take all eight mathematics courses in Problem 14.6, but only one per semester.

(*a*) Which choice or choices does she have for her first and for her last (eighth) semester?

(*b*) Suppose she wants to take Math 250 in her first year (first or second semester) and Math 340 in her senior year (seventh or eighth semester). Find all the ways that she can take the eight courses.

(*a*) By Fig. 14-11, Math 101 is the only minimal element and hence must be taken in the first semester, and Math 341 and 500 are the maximal elements and hence one of them must be taken in the last semester.

(*b*) Math 250 is not a minimal element and hence must be taken in the second semester, and Math 340 is not a maximal element so it must be taken in the seventh semester and Math 341 in the eighth semester. Also Math 500 must be taken in the sixth semester. The following gives the three possible ways to take the eight courses:

$$[101, 250, 251, 201, 450, 500, 340, 341]$$
$$[101, 250, 201, 251, 450, 500, 340, 341]$$
$$[101, 250, 201, 450, 251, 500, 340, 341]$$

UPPER AND LOWER BOUNDS, SUPREMUM AND INFIMUM

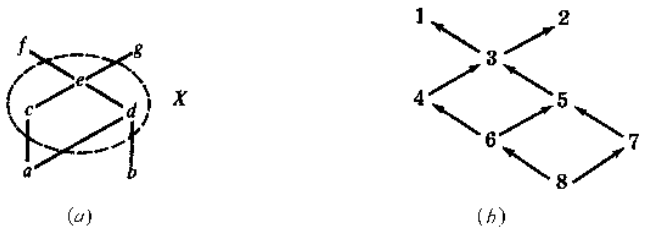
14.18. Let $S = \{a, b, c, d, e, f, g\}$ be ordered as in Fig. 14-14(*a*), and let $X = \{c, d, e\}$.

(*a*) Find the upper and lower bounds of X.

(*b*) Identify $\sup(X)$, the supremum of X, and $\inf(X)$, the infimum of X, if either exists.

The elements e, f, and g succeed every element of X; hence e, f, and g are the upper bounds of X. The element a precedes every element of X; hence it is the lower bound of X. Note that b is not a lower bound since b does not precede c; in fact, b and c are not comparable.

Since e precedes both f and g, we have $e = \sup(X)$. Likewise, since a precedes (trivially) every lower bound of X, we have $a = \inf(X)$. Note that $\sup(X)$ belongs to X but $\inf(X)$ does not belong to X.



(*a*) (*b*)

Fig. 14-14

14.19. Let $S = \{1, 2, 3, \ldots, 8\}$ be ordered as in Fig. 14-14(*b*), and let $A = \{2, 3, 6\}$.

(*a*) Find the upper and lower bounds of A.

(*b*) Identify $\sup(A)$ and $\inf(A)$ if either exists.

(*a*) The upper bound is 2, and the lower bounds are 6 and 8.

(*b*) Here $\sup(A) = 2$ and $\inf(A) = 6$.

14.20. Repeat Problem 14.19 for the subset $B = \{1, 2, 5\}$.

(*a*) There is no upper bound for B since no element succeeds both 1 and 2. The lower bounds are 6, 7, 8.

(*b*) Trivially, $\sup(A)$ does not exist since there are no upper bounds. Although A has three lower bounds, $\inf(A)$ does not exist since no lower bound succeeds both 6 and 7.

14.21. Consider the set $\mathbf{Q}$ of rational numbers with the usual order $\leq$, and consider the subset D of $\mathbf{Q}$ defined by

$$D = \{x : x \in \mathbf{Q} \text{ and } 8 < x^3 < 15\}$$

(*a*) Is D bounded above or below? (*b*) Do $\sup(D)$ and $\inf(D)$ exist?

(*a*) The subset D is bounded both above and below. For example, 1 is a lower bound and 100 an upper bound.

(*b*) $\sup(D)$ does not exist. Suppose, on the contrary, $\sup(D) = x$. Since $\sqrt[3]{15}$ is irrational, $x > \sqrt[3]{15}$. However, there exists a rational number y such that $\sqrt[3]{15} < y < x$. Thus y is also an upper bound for D. This contradicts the assumption that $x = \sup(D)$. On the other hand, $\inf(D)$ does exist. Specifically, $\inf(D) = 2$.

ISOMORPHIC (SIMILAR) SETS, SIMILARITY MAPPINGS

14.22. Suppose a poset A is isomorphic (similar) to a poset B and $f: A \to B$ is a similarity mapping. Are the following statements true or false?

(*a*) An element $a \in A$ is a first (last, minimal, or maximal) element of A if and only if $f(a)$ is a first (last, minimal, or maximal) element of B.

(*b*) An element $a \in A$ immediately precedes an element $a' \in A$, that is, $a \ll a'$, if and only if $f(a) \ll f(a')$.

(*c*) An element $a \in A$ has r immediate successors in A if and only if $f(a)$ has r immediate successors in B.

All the statements are true; the order structure of A is the same as the order structure of B.

14.23. Let S be the ordered set in Fig. 14-13. Suppose $A = \{1, 2, 3, 4, 5\}$ is isomorphic to S and

$$f = \{(a, 1), (b, 3), (c, 5), (d, 2), (e, 4)\}$$

is a similarity mapping from S to A. Draw the Hasse diagram of A.

The similarity mapping f preserves the order structure of S and hence f may be viewed simply as a relabeling of the vertices in the diagram of S. Thus Fig. 14-15 shows the Hasse diagram of A.

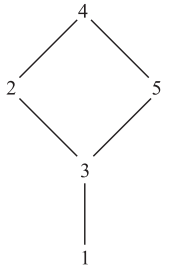


Fig. 14-15

14.24. Let $A = \{1, 2, 3, 4, 5, \}$ be ordered as in Fig. 14-15. Find the number n of similarity mappings $f: A \to A$.

Since 1 is the only minimal element of A and 4 is the only maximal element, we must have $f(1) = 1$ and $f(4) = 4$. Also, $f(3) = 3$ since 3 is the only immediate successor of 1. On the other hand, there are two possibilities for $f(2)$ and $f(5)$, that is, we can have $f(2) = 2$ and $f(5) = 5$, or $f(2) = 5$ and $f(5) = 2$. Accordingly, $n = 2$.

14.25. Give an example of a finite nonlinearly ordered set $X = (A, R)$ which is isomorphic to $Y = (A, R^{-1})$, the set A with the inverse order.

Let R be the partial ordering of $A = \{a, b, c, d, e\}$ pictured in Fig. 14-16(a). Then Fig. 14-16(b) shows A with the inverse order R^{-1}. (The diagram of R is simply turned upside down to obtain R^{-1}.) Notice that the two diagrams are identical except for the labeling.

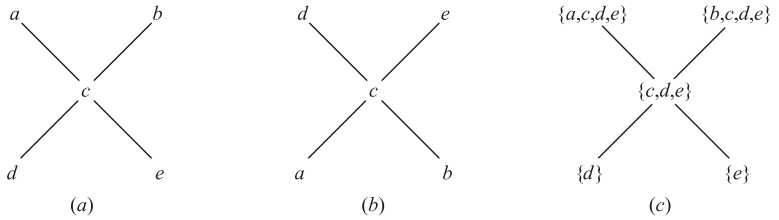


Fig. 14-16

14.26. Let A be an ordered set and, for each $a \in A$, let $p(a)$ denote the set of predecessors of a:

$$p(a) = \{x: x \precsim a\}$$

(called the *predecessor set* of a). Let $p(A)$ denote the collection of all predecessor sets of the elements in A ordered by set inclusion.

(a) Show that A and $p(A)$ are isomorphic by showing that the map $f: A \to p(A)$, defined by $f(a) = p(a)$, is a similarity mapping of A onto $p(A)$.

(b) Find the Hasse diagram of $p(A)$ for the set A in Fig. 14-16(a).

(a) First we show that f preserves the order relation of A. Suppose $a \precsim b$. Let $x \in p(a)$. Then $x \precsim a$, and hence $x \precsim b$; so $x \in p(b)$. Thus $p(a) \subseteq p(b)$. Suppose $a \parallel b$ (noncomparable). Then $a \in p(a)$ but $a \notin p(b)$; hence $p(a) \not\subseteq p(b)$. Similarly, $b \in p(b)$ but $b \notin p(a)$; hence $p(b) \not\subseteq p(a)$. Therefore, $p(a) \parallel p(b)$. Thus f preserves order.

We now need only show that f is one-to-one and onto. Suppose $y \in p(A)$. Then $y = p(a)$ for some $a \in A$. Thus $f(a) = p(a) = y$ so f is onto $p(A)$. Suppose $a \neq b$. Then $a \prec b$, $b \prec a$ or $a \parallel b$. In the first and third cases, $b \in p(b)$ but $b \notin p(a)$, and in the second case $a \in p(a)$ but $a \notin p(b)$. Accordingly, in all three cases, we have $p(a) \neq p(b)$. Therefore f is one-to-one.

Consequently, f is a similarity mapping of A onto $p(A)$ and so $A \simeq p(A)$.

(*b*) The elements of $p(A)$ follow:

$$p(a) = \{a, c, d, e\}, \qquad p(b) = \{b, c, d, e\}, \qquad p(c) = \{c, d, e\}, \qquad p(d) = \{d\}, \qquad p(e) = \{e\}$$

Figure 14-16(*c*) gives the diagram of $p(A)$ ordered by set inclusion. Observe that the diagrams in Fig. 14-16(*a*) and (*c*) are identical except for the labeling of the vertices.

WELL-ORDERED SETS

14.27. Prove the Principle of Transfinite Induction: Let A be a subset of a well-ordered set S with the following two properties: (i) $a_0 \in A$. (ii) If $s(a) \subseteq A$ then $a \in A$. Then $A = S$.

(Here a_0 is the first element of A, and $s(a)$ is the initial segment of a, i.e., the set of all elements strictly preceding a.) Suppose $A \neq S$. Let $B = S \backslash A$. Then $B \neq \varnothing$. Since S is well-ordered, B has a first element b_0. Each element $x \in s(b_0)$ precedes b_0 and hence does not belong to B. Thus every $x \in s(b_0)$ belongs to A; hence $s(b_0) \subseteq A$. By (ii), $b_0 \in A$. This contradicts the assumption that $b_0 \in S \backslash A$. Thus the original assumption that $A \neq S$ is not true; in other words $A = S$.

14.28. Let S be a well-ordered set with first element a_0. Define a *limit element* of S.

An element $b \in S$ is a limit element if $b \neq a_0$ and b has no immediate predecessor.

14.29. Let $S = (\mathbf{N}, \precsim)$ be ordered as in Problem 14.8. (See Fig. 14-12.) Does S have any limit elements?

As indicated by Fig. 14-12, every power of 2, that is, $1, 2, 4, 8, \ldots$, has no immediate predecessor, and hence is a limit element of S.

14.30. Let S be a well-ordered set. Let $f: S \to S$ be a similarity mapping of S into S. Prove that, for every $a \in S$, we have $a \precsim f(a)$.

Let $D = \{x : f(x) \prec x\}$. If D is empty, then the statement is true. Suppose $D \neq \varnothing$. Since D is well-ordered, D has a first element, say d_0. Since $d_0 \in D$, we have $f(d_0) \prec d_0$. Since f is a similarity mapping:

$$f(d_0) \prec d_0 \qquad \text{implies} \qquad f(f(d_0)) \prec f(d_0)$$

Thus $f(d_0)$ also belongs to D. But $f(d_0) \prec d_0$ and $f(d_0) \in D$ contradicts the fact that d_0 is the first element of D. Hence the original assumption that $D \neq \varnothing$ leads to a contradiction. Therefore D is empty and the statement is true.

14.31. Let A be a well-ordered set. Let $s(A)$ denote the collection of all initial segments $s(a)$ of elements $a \in A$ ordered by set inclusion. Prove A is isomorphic to $s(A)$ by showing that the map $f: A \to s(A)$, defined by $f(a) = s(a)$, is a similarity mapping of A onto $s(A)$. (Compare with Problem 14.26.)

First we show that f is one-to-one and onto. Suppose $y \in s(A)$. Then $y = s(a)$ for some $a \in A$. Thus $f(a) = s(a) = y$, so f is onto $s(A)$. Suppose $x \neq y$. Then one precedes the other, say, $x \prec y$. Then $x \in s(y)$. But $x \notin s(x)$. Thus $s(x) \neq s(y)$. Therefore, f is also one-to-one.

We now need only show that f preserves order, that is,

$$x \precsim y \qquad \text{if and only if} \qquad s(x) \subseteq s(y)$$

Suppose $x \precsim y$. If $a \in s(x)$, then $a \prec x$ and hence $a \prec y$; thus $a \in s(y)$. Thus $s(x) \subseteq s(y)$. On the other hand, suppose $x \not\precsim y$, that is, $x \succ y$. Then $y \in s(x)$. But $y \notin s(y)$; hence $s(x) \not\subseteq s(y)$. In other words, $x \precsim y$ if and only if $s(x) \subseteq s(y)$.

Accordingly, f is a similarity mapping of A onto $S(A)$, and so $A \simeq s(A)$.

LATTICES

14.32. Write the dual of each statement:

(*a*) $(a \wedge b) \vee c = (b \vee c) \wedge (c \vee a)$; (*b*) $(a \wedge b) \vee a = a \wedge (b \vee a)$.

Replace $\vee$ by $\wedge$ and $\wedge$ by $\vee$ in each statement to obtain the dual statement:

(*a*) $(a \vee b) \wedge c = (b \wedge c) \vee (c \wedge a)$.

(*b*) $(a \vee b) \wedge a = a \vee (b \wedge a)$.

14.33. Give an example of an infinite lattice L with finite length.

Let $L = \{0, 1, a_1, a_2, a_3, \ldots\}$ and let L be ordered as in Fig. 14-17; that is, for each $n \in \mathbf{N}$, we have

$$0 < a_n < 1$$

Then L has finite length since L has no infinite linearly ordered subset.

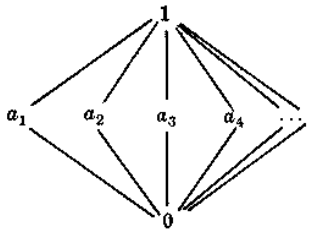


Fig. 14-17

14.34. Prove Theorem 14.4: Let L be a lattice. Then: (i) $a \wedge b = a$ if and only if $a \vee b = b$. (ii) The relation $a \precsim b$ (defined by $a \wedge b = a$ or $a \vee b = b$) is a partial order on L.

(i) Suppose $a \wedge b = a$. Using the absorption law in the first step we have:

$$b = b \vee (b \wedge a) = b \vee (a \wedge b) = b \vee a = a \vee b$$

Now suppose $a \vee b = b$. Again using the absorption law in the first step we have:

$$a = a \wedge (a \vee b) = a \wedge b$$

Thus $a \wedge b = a$ if and only if $a \vee b = b$.

(ii) For any a in L, we have $a \wedge a = a$ by idempotency. Hence $a \precsim a$, and so $\precsim$ is reflexive.

Suppose $a \precsim b$ and $b \precsim a$. Then $a \wedge b = a$ and $b \wedge a = b$. Therefore, $a = a \wedge b = b \wedge a = b$, and so $\precsim$ is antisymmetric.

Lastly, suppose $a \precsim b$ and $b \precsim c$. Then $a \wedge b = a$ and $b \wedge c = b$. Thus

$$a \wedge c = (a \wedge b) \wedge c = a \wedge (b \wedge c) = a \wedge b = a$$

Therefore $a \precsim c$, and so $\precsim$ is transitive. Accordingly, $\precsim$ is a partial order on L.

14.35. Which of the partially ordered sets in Fig. 14-18 are lattices?

A partially ordered set is a lattice if and only if $\sup(x, y)$ and $\inf(x, y)$ exist for each pair x, y in the set. Only (c) is not a lattice since $\{a, b\}$ has three upper bounds, c, d and I, and no one of them precedes the other two, i.e., $\sup(a, b)$ does not exist.

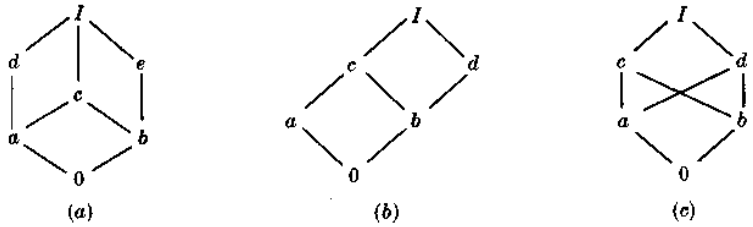


Fig. 14-18

14.36. Consider the lattice L in Fig. 14-18(a).

(a) Which nonzero elements are join irreducible?

(b) Which elements are atoms?

(c) Which of the following are sublattices of L:

$$L_1 = \{0, a, b, I\}, \qquad L_2 = \{0, a, e, I\}$$
$$L_3 = \{a, c, d, I\}, \qquad L_4 = \{0, c, d, I\}$$

(d) Is L distributive?

(e) Find complements, if they exist, for the elements, a, b and c.

(f) Is L a complemented lattice?

(a) Those nonzero elements with a unique immediate predecessor are join irreducible. Hence a, b, d, and e are join irreducible.

(b) Those elements which immediately succeed 0 are atoms, hence a and b are the atoms.

(c) A subset L' is a sublattice if it is closed under $\wedge$ and $\vee$. L_1 is not a sublattice since $a \vee b = c$, which does not belong to L_1. The set L_4 is not a sublattice since $c \wedge d = a$ does not belong to L_4. The other two sets, L_2 and L_3, are sublattices.

(d) L is not distributive since $M = \{0, a, d, e, I\}$ is a sublattice which is isomorphic to the nondistributive lattice in Fig. 14-7(a).

(e) We have $a \wedge e = 0$ and $a \vee e = I$, so a and e are complements. Also b and d are complements. However, c has no complement.

(f) L is not a complemented lattice since c has no complement.

14.37. Consider the lattice M in Fig. 14-18(b).

(a) Find the nonzero join irreducible elements and atoms of M.

(b) Is M distributive?

(c) Is M complemented?

(a) The nonzero elements with a unique predecessor are a, b, and d, and of these three only a and b are atoms since their unique predecessor is 0.

(b) M is distributive since M does not have a sublattice isomorphic to one of the lattices in Fig. 14-7.

(*c*) M is not complemented since b has no complement. Note a is the only solution to $b \wedge x = 0$ but $b \vee a = c \neq I$.

14.38. Prove Theorem 14.8: Let L be a finite distributive lattice. Then every a in L can be written uniquely (except for order) as the join of irredundant join irreducible elements.

Since L is finite we can write a as the join of irredundant join irreducible elements as we discussed in Section 14.9. Thus we need to prove uniqueness. Suppose

$$a = b_1 \vee b_2 \vee \cdots \vee b_r = c_1 \vee c_2 \vee \cdots \vee c_s$$

where the b's are irredundant and join irreducible and the c's are irredundant and irreducible. For any given i we have

$$b_i \precsim (b_1 \vee b_2 \vee \cdots \vee b_r) = (c_1 \vee c_2 \vee \cdots \vee c_s)$$

Hence

$$b_i = b_i \wedge (c_1 \vee c_2 \vee \cdots \vee c_s) = (b_i \wedge c_1) \vee (b_i \wedge c_2) \vee \cdots \vee (b_i \wedge c_s)$$

Since b_i is join irreducible, there exists a j such that $b_i = b_i \wedge c_j$, and so $b_i \precsim c_j$. By a similar argument, for c_j there exists a b_k such that $c_j \precsim b_k$. Therefore

$$b_i \precsim c_j \precsim b_k$$

which gives $b_i = c_j = b_k$ since the b's are irredundant. Accordingly, the b's and c's may be paired off. Thus the representation for a is unique except for order.

14.39. Prove Theorem 14.10: Let L be a complemented lattice with unique complements. Then the join irreducible elements of L, other than 0, are its atoms.

Suppose a is join irreducible and is not an atom. Then a has a unique immediate predecessor $b \neq 0$. Let b' be the complement of b. Since $b \neq 0$ we have $b' \neq I$. If a precedes b', then $b \precsim a \precsim b'$, and so $b \wedge b' = b'$, which is impossible since $b \wedge b' = I$. Thus a does not precede b', and so $a \wedge b'$ must strictly precede a. Since b is the unique immediate predecessor of a, we also have that $a \wedge b'$ precedes b as in Fig. 14-19. But $a \wedge b'$ precedes b'. Hence

$$a \wedge b' \precsim \inf(b, b') = b \wedge b' = 0$$

Thus $a \wedge b' = 0$. Since $a \vee b = a$, we also have that

$$a \vee b' = (a \vee b) \vee b' = a \vee (b \vee b') = a \vee I = I$$

Therefore b' is a complement of a. Since complements are unique, $a = b$. This contradicts the assumption that b is an immediate predecessor of a. Thus the only join irreducible elements of L are its atoms.

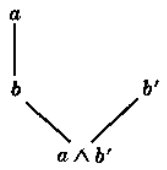


Fig. 14-19

Supplementary Problems

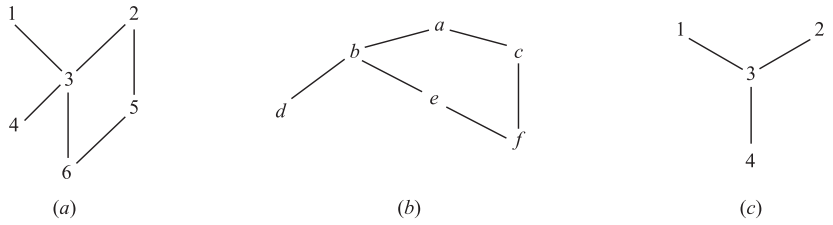
ORDERED SETS AND SUBSETS

14.40. Let $A = \{1, 2, 3, 4, 5, 6\}$ be ordered as in Fig. 14-20(a).

(a) Find all minimal and maximal elements of A.

(b) Does A have a first or last element?

(c) Find all linearly ordered subsets of A, each of which contains at least three elements.



(a) (b) (c)

Fig. 14-20

14.41. Let $B = \{a, b, c, d, e, f\}$ be ordered as in Fig. 14-20(b).

(a) Find all minimal and maximal elements of B.

(b) Does B have a first or last element?

(c) List two and find the number of consistent enumerations of B into the set $\{1, 2, 3, 4, 5, 6\}$.

14.42. Let $C = \{1, 2, 3, 4\}$ be ordered as in Fig. 14-20(c). Let $L(C)$ denote the collection of all nonempty linearly ordered subsets of C ordered by set inclusion. Draw a diagram of $L(C)$.

14.43. Draw the diagrams of the partitions of m (see Example 14.14) where: (a) $m = 4$; (b) $m = 6$.

14.44. Let $\mathbf{D}_m$ denote the positive divisors of m ordered by divisibility. Draw the Hasse diagrams of: (a) $\mathbf{D}_{12}$; (b) $\mathbf{D}_{15}$; (c) $\mathbf{D}_{16}$; (d) $\mathbf{D}_{17}$.

14.45. Let $S = \{a, b, c, d, e, f\}$ be a poset. Suppose there are exactly six pairs of elements such that the first immediately precedes the second as follows:

$$f \ll a, \quad f \ll d, \quad e \ll b, \quad c \ll lf, \quad e \ll c, \quad b \ll f$$

(a) Find all minimal and maximal elements of S.

(b) Does S have any first or last element?

(c) Find all pairs of elements, if any, which are noncomparable.

14.46. State whether each of the following is true or false and, if it is false, give a counterexample.

(a) If a poset S has only one maximal element a, then a is a last element.

(b) If a finite poset S has only one maximal element a, then a is a last element.

(c) If a linearly ordered set S has only one maximal element a, then a is a last element.

14.47. Let $S = \{a, b, c, d, e\}$ be ordered as in Fig. 14-21(a).

(a) Find all minimal and maximal elements of S.

(b) Does S have any first or last element?

(c) Find all subsets of S in which c is a minimal element.

(d) Find all subsets of S in which c is a first element.

(e) List all linearly ordered subsets with three or more elements

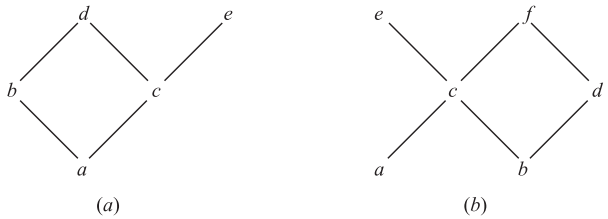


Fig. 14-21

14.48. Let $S = \{a, b, c, d, e, f\}$ be ordered as in Fig. 14-21(b).

(a) Find all minimal and maximal elements of S.

(b) Does S have any first or last element?

(c) List all linearly ordered subsets with three or more elements.

14.49. Let $S = \{a, b, c, d, e, f, g\}$ be ordered as in Fig. 14-14(a). Find the number n of linearly ordered subsets of S with: (a) four elements; (b) five elements.

14.50. Let $S = \{1, 2, \ldots, 7, 8\}$ be ordered as in Fig. 14-14(b). Find the number n of linearly ordered subsets of S with: (a) five elements; (b) six elements.

CONSISTENT ENUMERATIONS

14.51. Let $S = \{a, b, c, d, e\}$ be ordered as in Fig. 14-21(a). List all consistent enumerations of S into $\{1, 2, 3, 4, 5\}$.

14.52. Let $S = \{a, b, c, d, e, f\}$ be ordered as in Fig. 14-21(b). Find the number n of consistent enumerations of S into $\{1, 2, 3, 4, 5, 6\}$.

14.53. Suppose the following are three consistent enumerations of an ordered set $A = \{a, b, c, d\}$:

$$[(a,1),(b,2),(c,3),(d,4)], \qquad [(a,1),(b,3),(c,2),(d,4)], \qquad [(a,1),(b,4),(c,2),(d,3)]$$

Assuming the Hasse diagram D of A is connected, draw D.

ORDER AND PRODUCT SETS AND KLEENE CLOSURES

14.54. Let $M = \{2, 3, 4, \ldots, \}$ and let $M^2 = M \times M$ be ordered as follows:

$$(a, b) \precsim (c, d) \qquad \text{if } a \mid c \text{ and } b \leq d$$

Find all minimal and maximal elements of $M \times M$.

14.55. Consider the English alphabet $A = \{a, b, c, \ldots, y, z\}$ with the usual (alphabetical) order. Recall that the Kleene closure A^* consists of all words in **A**. Let L consist of the following elements in A^*:

gone, or, arm, go, an, about, gate, one, at, occur

(a) Sort L according to the short-lex order, i.e., first by length and then alphabetically.

(b) Sort L alphabetically.

14.56. Consider the ordered sets A and B appearing in Fig. 14-20(a) and (b), respectively. Suppose $S = A \times B$ is given the product order, i.e.,

$$(a, b) \precsim (a', b') \qquad \text{if } a \precsim a' \text{ and } b \precsim b'$$

Insert the correct symbol, $\prec$, $\succ$, or $\|$, between each pair of elements of S:

(a) $(4, b)$ ____ $(2, e)$ (b) $(3, a)$ ____ $(6, f)$

(c) $(5, d)$ ____ $(1, a)$ (d) $(6, e)$ ____ $(2, b)$

14.57. Suppose $\mathbf{N} = \{1, 2, 3, \ldots\}$ and $\mathbf{A} = \{a, b, c, \ldots, y, z\}$ are given the usual orders, and $S = \mathbf{N} \times \mathbf{A}$ is ordered lexicographically. Sort the following elements of S:

$$(2, z), \quad (1, c), \quad (2, c), \quad (1, y), \quad (4, b), \quad (4, z), \quad (3, b) \quad (2, a)$$

UPPER AND LOWER BOUNDS, SUPREMUM AND INFIMUM

14.58. Let $S = \{a, b, c, d, e, f, g\}$ be ordered as in Fig. 14-14(a). Consider the subset $A = \{a, c, d\}$ of S.

(a) Find the set of upper bounds of A. (c) Does $\sup(A)$ exist?

(b) Find the set of lower bounds of A. (d) Does $\inf(A)$ exist?

14.59. Repeat Problem 14.58 for subset $B = \{b, c, e\}$ of S.

14.60. Let $S = \{1, 2, \ldots, 7, 8\}$ be ordered as in Fig. 14-14(b). Consider the subset $A = \{3, 6, 7\}$ of S.

(a) Find the set of upper bounds of A. (c) Does $\sup(A)$ exist?

(b) Find the set of lower bounds of A. (d) Does $\inf(A)$ exist?

14.61. Repeat Problem 14.60 for the subset $B = \{1, 2, 4, 7\}$ of S.

14.62. Consider the set $\mathbf{Q}$ of rational numbers with the usual order $\leq$. Let $A = \{x : x \in \mathbf{Q} \text{ and } 5 < x^3 < 27\}$.

(a) Is A bounded above or below?

(b) Do $\sup(A)$ and $\inf(A)$ exist?

14.63. Consider the set $\mathbf{R}$ of real numbers with the usual order $\leq$. Let $A = \{x : x \in \mathbf{Q} \text{ and } 5 < x^3 < 27\}$.

(a) Is A bounded above or below?

(b) Do $\sup(A)$ and $\inf(A)$ exist?

ISOMORPHIC (SIMILAR) SETS, SIMILARITY MAPPINGS

14.64. Let S be the ordered set in Fig. 14-21(a). Suppose $A = \{1, 2, 3, 4, 5\}$ is isomorphic to S and the following is a similarity mapping from S into A:

$$f = \{(a, 1), (b, 4), (c, 5), (d, 2), (e, 3)\}$$

Draw the Hasse diagram of A.

14.65. Find the number of nonisomorphic posets with three elements a, b, c, and draw their diagrams.

14.66. Find the number of connected nonisomorphic posets with four elements a, b, c, d, and draw their diagrams.

14.67. Find the number of similarity mappings $f : S \to S$ if S is the ordered set in: (a) Fig. 14-20(a); (b) Fig. 14-20(b); (c) Fig. 14-20(c).

14.68. Show that the isomorphism relation $A \simeq B$ for ordered sets is an equivalence relation, that is: (*a*) $A \simeq A$ for any ordered set A. (*b*) If $A \simeq B$, then $B \simeq A$. (*c*) If $A \simeq B$ and $B \simeq C$, then $A \simeq C$.

WELL-ORDERED SETS

14.69. Suppose the union S of the sets $A = \{a_1, a_2, a_3, \ldots\}$, $B = \{b_1, b_2, b_3, \ldots\}$, $C = \{c_1, c_2, c_3, \ldots\}$ is ordered as follows:

$$S = \{A;\ B;\ C\} = \{a_1, a_2, \ldots, b_1, b_2, \ldots, c_1, c_2, \ldots\}$$

(*a*) Show that S is well-ordered.

(*b*) Find all limit elements of S.

(*c*) Show that S is not isomorphic to $\mathbf{N} = \{1, 2, \ldots\}$ with the usual order $\leq$.

14.70. Let $A = \{a, b, c\}$ be linearly ordered by $a < b < c$, and let $\mathbf{N} = \{1, 2, \ldots\}$ be given the usual order $\leq$.

(*a*) Show that $S = \{A;\ \mathbf{N}\}$ is isomorphic to $\mathbf{N}$.

(*b*) Show that $S' = \{\mathbf{N};\ A\}$ is not isomorphic to $\mathbf{N}$.

14.71. Suppose A is a well-ordered set under the relation $\precsim$, and suppose A is also well-ordered under the inverse relation $\succsim$. Describe A.

14.72. Suppose A and B are well-ordered isomorphic sets. Show that there is only one similarity mapping $f: A \to B$.

14.73. Let S be a well-ordered set. For any $a \in S$, the set $s(a) = \{x: x \prec a\}$ is called an initial segment of a. Show that S cannot be isomorphic to one of its initial segments. (*Hint*: Use Problem 14.30.)

14.74. Suppose $s(a)$ and $s(b)$ are distinct initial segments of a well-ordered set S. Show that $s(a)$ and $s(b)$ cannot be isomorphic. (*Hint*: Use Problem 14.73.)

LATTICES

14.75. Consider the lattice L in Fig. 14-22(*a*). (*a*) Find all sublattices with five elements. (*b*) Find all join-irreducible elements and atoms. (*c*) Find complements of a and b, if they exist. (*d*) Is L distributive? Complemented?

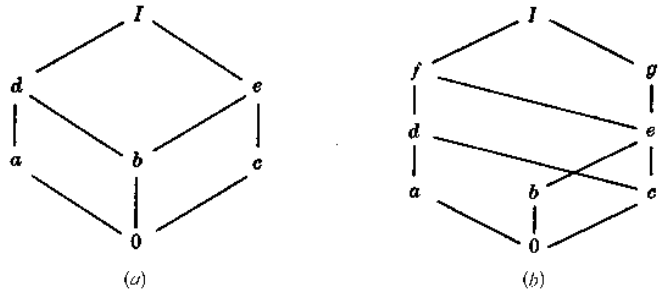


Fig. 14-22

14.76. Consider the lattice M in Fig. 14-22(*b*). (*a*) Find join-irreducible elements. (*b*) Find the atoms. (*c*) Find complements of a and b, if they exist. (*d*) Express each x in M as the join of irredundant join-irreducible elements. (*e*) Is M distributive? Complemented?

14.77. Consider the bounded lattice L in Fig. 14-23(a).

(a) Find the complements, if they exist, of e and f.

(b) Express I in an irredundant join irreducible decomposition in as many ways as possible.

(c) Is L distributive?

(d) Describe the isomorphisms of L with itself.

14.78. Consider the bounded lattice L in Fig. 14-23(b).

(a) Find the complements, if they exist, of a and f.

(b) Express I in an irredundant join irreducible decomposition in as many ways as possible.

(c) Is L distributive?

(d) Describe the isomorphisms of L with itself.

14.79. Consider the bounded lattice L in Fig. 14-23(c).

(a) Find the complements, if they exist, of a and c.

(b) Express I in an irredundant join irreducible decomposition in as many ways as possible.

(c) Is L distributive?

(d) Describe the isomorphisms of L with itself.

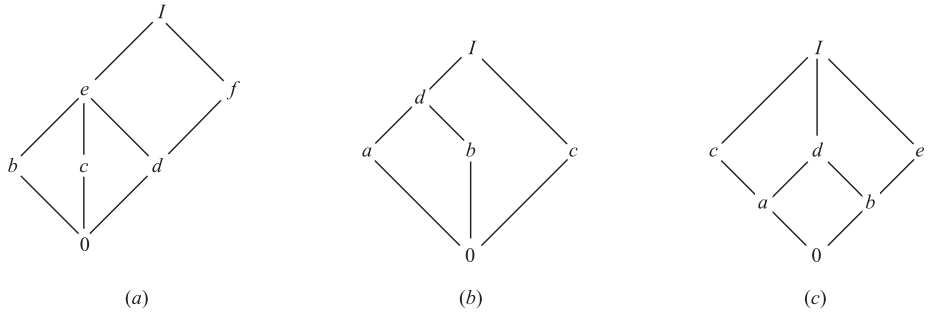


Fig. 14-23

14.80. Consider the lattice $\mathbf{D}_{60} = \{1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60\}$, the divisors of 60 ordered by divisibility. (a) Draw the diagram of $\mathbf{D}_{60}$. (b) Which elements are join irreducible? Atoms? (c) Find complements of 2 and 10, if they exist. (d) Express each number x as the join of a minimum number of irredundant join irreducible elements.

14.81. Consider the lattice $\mathbf{N}$ of positive integers ordered by divisibility. (a) Which elements are join irreducible? (b) Which elements are atoms?

14.82. Show that the following "weak" distributive laws hold for any lattice:

(a) $a \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c)$.

(b) $a \wedge (b \vee c) \geq (a \wedge b) \vee (a \wedge c)$.

14.83. Let $S = \{1, 2, 3, 4\}$. Using the notation [12,3,4] $\equiv$ [{1,2}, {3}, {4}], three partitions of S are:

$$P_1 = [12, 3, 4], \qquad P_2 = [12, 34], \qquad P_3 = [13, 2, 4]$$

(*a*) Find the other nine partitions of S.

(*b*) Let L be the collection of 12 partitions S ordered by *refinement*, i.e., $P_i \precsim P_j$ if each cell of P_i is a subset of a cell of P_j. For example $P_1 \precsim P_2$, but P_2 and P_3 are noncomparable. Show that L is a bounded lattice and draw its diagram.

14.84. An element a in a lattice L is said to be *meet-irreducible* if $a = x \wedge y$ implies $a = x$ or $a = y$. Find all meet-irreducible elements in: (*a*) Fig. 13-22(*a*); (*b*) Fig. 14-22(*b*); (*c*) $\mathbf{D}_{60}$ (see Problem 14.80).

14.85. A lattice M is said to be *modular* if whenever $a \leq c$ we have the law

$$a \vee (b \wedge c) = (a \vee b) \wedge c$$

(*a*) Prove that every distributive lattice is modular.

(*b*) Verify that the nondistributive lattice in Fig. 14-7(*b*) is modular; hence the converse of (*a*) is not true.

(*c*) Show that the nondistributive lattice in Fig. 14-7(*a*) is nonmodular. [In fact, one can prove that every nonmodular lattice contains a sublattice isomorphic to Fig. 14-7(*a*).]

14.86. Let R be a ring. Let L be the collection of all ideals of R. For any ideals J and K of R, we define:

$$J \vee K = J + K \qquad \text{and} \qquad J \wedge K = J \cap K$$

Prove that L is a bounded lattice.

Answers to Supplementary Problems

14.40. (*a*) Minimal, 4 and 6; maximal, 1 and 2. (*b*) First, none; last, none. (*c*) $\{1, 3, 4\}$, $\{1, 3, 6\}$, $\{2, 3, 4\}$, $\{2, 3, 6\}$, $\{2, 5, 6\}$.

14.41. (*a*) Minimal, d and f; maximal, a. (*b*) First, none; last, a. (*c*) There are eleven: *dfebca*, *dfecba*, *dfceba*, *fdebca*, *fdecba*, *fdceba*, *fedbca*, *fedcba*, *fcdeba*, *fecdba*, *fcedba*.

14.42. See Fig. 14-24.

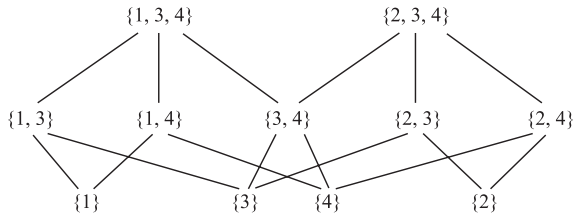


Fig. 14-24

14.43. See Fig. 14-25.

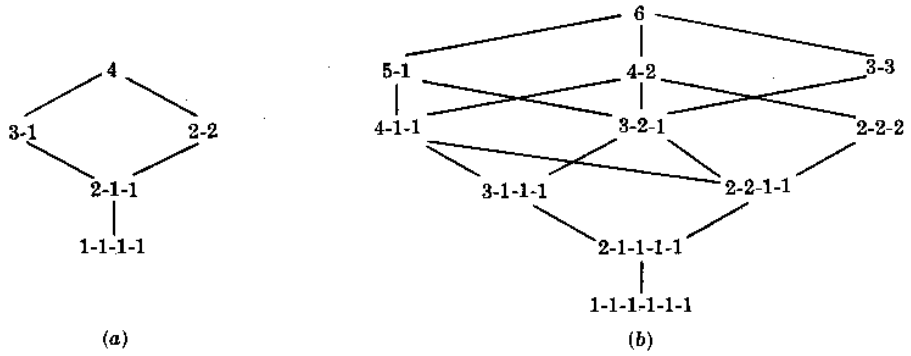


Fig. 14-25

14.44. See Fig. 14-26.

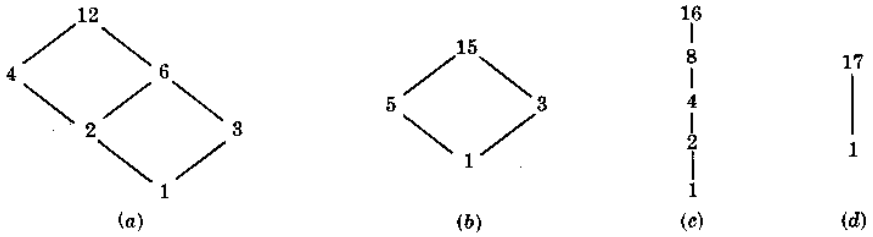


Fig. 14-26

14.45. *Hint*: Draw the diagram of S. (*a*) Minimal, e; maximal, a, d. (*b*) First, e; Last, none. (*c*) $\{a, d\}$, $\{b, c\}$.

14.46. (*a*) False. Example: $\mathbf{N} \cup \{a\}$ where $1 \ll a$, and $\mathbf{N}$ ordered by $\leq$. (*b*) True. (*c*) True.

14.47. (*a*) Minimal, a; maximal, d and e. (*b*) First, a; last, none. (*c*) Any subset which contains c and omits a; that is: c, cb, cd, ce, cbd, cbe, cde, $cbde$. (*d*) c, cd, ce, cde. (*e*) abd, acd, ace.

14.48. (*a*) Minimal, a and b; maximal, e and f. (*b*) First, none; last, none. (*c*) ace, acf, bce, bcf, bdf.

14.49. (*a*) Four. (*b*) None.

14.50. (*a*) Six. (*b*) None.

14.51. *abcde*, *abced*, *acbde*, *acbed*, *acebd*.

14.52. Eleven.

14.53. $a \ll b$, $a \ll c$, $c \ll d$.

14.54. Minimal, $(p, 2)$ where p is a prime. Maximal, none.

14.55. (*a*) an, at, go, or, arm, one, gate, gone, about, occur.
(*b*) an, about, arm, at, gate, go, gone, occur, one, or.

14.56. (*a*) $\|$; (*b*) $>$; (*c*) $\|$; (*d*) $<$.

14.57. $1c$, $1y$, $2a$, $2c$, $2z$, $3b$, $4b$, $4z$

14.58. (*a*) e, f, g; (*b*) a; (*c*) $\sup(A) = e$; (*d*) $\inf(A) = a$.

14.59. (*a*) e, f, g; (*b*) none; (*c*) $\sup(B) = e$; (*d*) none.

14.60. (*a*) 1, 2, 3; (*b*) 8; (*c*) $\sup(A) = 3$; (*d*) $\inf(A) = 8$.

14.61. (*a*) None; (*b*) 8; (*c*) none; (*d*) $\inf(B) = 8$.

14.62. (*a*) Both; (*b*) $\sup(A) = 3$; $\inf(A)$ does not exist.

14.63. (*a*) Both; (*b*) $\sup(A) = 3$; $\inf(A) = \sqrt[3]{5}$.

14.64. See Fig. 14-27.

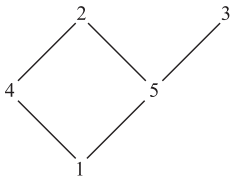


Fig. 14-27

14.65. Four: (1) a, b, c; (2) $a, b \ll c$; (3) $a \ll b$, $a \ll c$; (4) $a \ll b \ll c$.

14.66. Four: See Fig. 14-28.

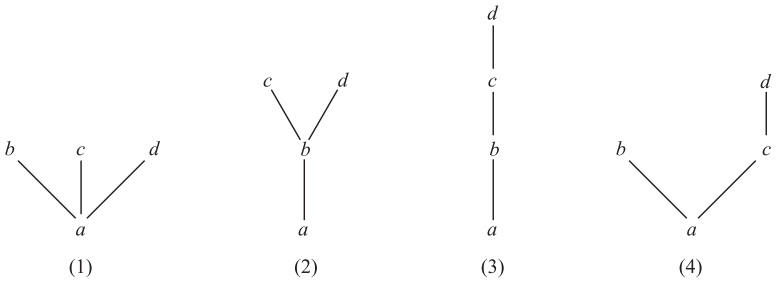


Fig. 14-28

14.67. (*a*) One: identity mapping; (*b*) one; (*c*) two.

14.69. (*b*) b_1, c_1. (*c*) **N** has no limit points.

14.70. (*a*) Define $f: S \to N$ by $f(a) = 1, f(b) = 2, f(3) = 3, f(n) = n + 3$.
(*b*) The element a is a limit point of S', but **N** has no limit points.

14.71. A is a finite linearly ordered set.

14.75. (*a*) Six: $0abdI$, $0acdI$, $0adeI$, $0bceI$, $0aceI$, $0cdeI$.
(*b*) (i) $a, b, e, 0$; (*b*) (ii) a, b, c.
(*c*) c and e are complements of a. b has no complement.
(*d*) No. No.

14.76. (*a*) $a, b, c, g, 0$. (*b*) a, b, c. (*c*) a: g; b: none.
(*d*) $I = a \vee g, f = a \vee b = a \vee c, e = b \vee c, d = a \vee c$. Other elements are join irreducible. (*e*) No. No.

14.77. (*a*) e has none; f has b and c.
(*b*) $I = c \vee d \vee f = b \vee c \vee f = b \vee d \vee f$.
(*c*) No, since decompositions are not unique.
(*d*) Two: 0, d, e, f, I must be mapped into themselves. Then $F = 1_L$, identity map on L, or $F = \{(b, c), (c, b)\}$.

14.78. (*a*) a has c; c has a and b. (*b*) $I = a \vee c = b \vee c$.
(*c*) No. (*d*) Two: 0, c, d, I must be mapped into themselves. Then $f = 1_L$ or $f = \{(a, b), (b, a)\}$.

14.79. (*a*) a has e, c has b and e. (*b*) $I = a \vee e = b \vee c = c \vee e$.
(*c*) No. (*d*) Two: 0, d, I are mapped into themselves. Then $f = 1_L$ or $f = \{(a, b), (b, a), (c, d), (d, c)\}$

14.80. (*a*) See Fig. 14-29. (*b*) 1, 2, 3, 4, 5. The atoms are 2, 3 and 5. (*c*) 2 has none, 10 has 3.
(*d*) $60 = 4 \vee 3 \vee 5$, $30 = 2 \vee 3 \vee 5$, $20 = 4 \vee 5$; $15 = 3 \vee 5$, $12 = 3 \vee 4$, $10 = 2 \vee 5$, $6 = 2 \vee 3$.

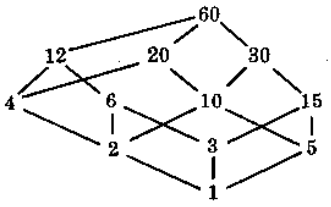


Fig. 14-29

14.81. (*a*) Powers of primes and 1; (*b*) primes.

14.83. (*a*) $[1,2,3,4]$, $[14,2,3]$, $[13,24]$, $[14,23]$, $[123,4]$, $[124,3]$, $[134,2]$, $[234,1]$, $[1234]$.

(*b*) See Fig. 14-30.

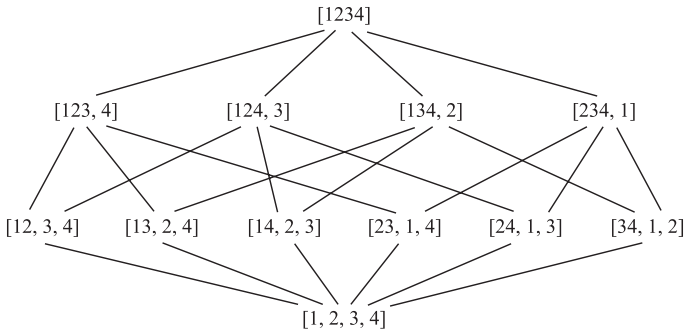


Fig. 14-30

14.84. Geometrically, an element $a \neq I$ is meet-irreducible if and only if a has only one immediate successor. (*a*) a, c, d, e, I; (*b*) a, b, d, f, g, I; (*c*) 4, 6, 10, 12, 15, 60.

14.85. (*a*) If $a \leq c$ then $a \vee c = c$. Hence

$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c) = (a \vee b) \wedge c$$

(*c*) Here $a \leq c$. But $a \vee (b \wedge c) = a \vee 0 = a$ and $(a \vee b) \wedge c = I \wedge c = c$; hence

$$a \vee (b \wedge c) \neq (a \vee b) \wedge c.$$

© The McGraw–Hill Companies, 2004

Chapter 15

Boolean Algebra

15.1 INTRODUCTION

Both sets and propositions satisfy similar laws, which are listed in Tables 1-1 and 4-1 (in Chapters 1 and 4, respectively). These laws are used to define an abstract mathematical structure called a *Boolean algebra*, which is named after the mathematician George Boole (1813–1864).

15.2 BASIC DEFINITIONS

Let B be a nonempty set with two binary operations $+$ and $*$, a unary operation $'$, and two distinct elements 0 and 1. Then B is called a *Boolean algebra* if the following axioms hold where a, b, c are any elements in B:

$[\mathbf{B}_1]$ Commutative laws:
$(1a)\quad a+b=b+a$ $\qquad$ $(1b)\quad a*b=b*a$

$[\mathbf{B}_2]$ Distributive laws:
$(2a)\quad a+(b*c)=(a+b)*(a+c)$ $\qquad$ $(2b)\quad a*(b+c)=(a*b)+(a*c)$

$[\mathbf{B}_3]$ Identity laws:
$(3a)\quad a+0=a$ $\qquad$ $(3b)\quad a*1=a$

$[\mathbf{B}_4]$ Complement laws:
$(4a)\quad a+a'=1$ $\qquad$ $(4b)\quad a*a'=0$

We will sometimes designate a Boolean algebra by $\langle B,+,*,',0,1\rangle$ when we want to emphasize its six parts. We say 0 is the *zero* element, 1, is the *unit* element, and a' is the *complement* of a. We will usually drop the symbol $*$ and use juxtaposition instead. Then $(2b)$ is written $a(b+c)=ab+ac$ which is the familiar algebraic identity of rings and fields. However, $(2a)$ becomes $a+bc=(a+b)(a+c)$, which is certainly not a usual identity in algebra.

The operations $+$, $*$, and $'$ are called sum, product, and complement, respectively. We adopt the usual convention that, unless we are guided by parentheses, $'$ has precedence over $*$, and $*$ has precedence over $+$. For example,

$$a+b*c \text{ means } a+(b*c) \text{ and not } (a+b)*c \qquad a*b' \text{ means } a*(b') \text{ and not } (a*b)'$$

Of course when $a+b*c$ is written $a+bc$ then the meaning is clear.

EXAMPLE 15.1

(*a*) Let $\mathbf{B}=\{0,1\}$, the set of *bits* (binary digits), with the binary operations of $+$ and $*$ and the unary operation $'$ defined by Fig. 15-1. Then $\mathbf{B}$ is a Boolean algebra. (Note $'$ simply changes the bit, i.e., $1'=0$ and $0'=1$.)

$+$	1	0
1	1	1
0	1	0

$*$	1	0
1	1	0
0	0	0

$'$	1	0
	0	1

Fig. 15-1

(*b*) Let $\mathbf{B}^n=\mathbf{B}\times\mathbf{B}\times\cdots\times\mathbf{B}$ (n factors) where the operations of $+$, $*$, and $'$ are defined componentwise using Fig. 15-1. For notational convenience, we write the elements of $\mathbf{B}^n$ as n-bit sequences without commas, e.g., $x=110011$ and $y=111000$ belong to $\mathbf{B}^6$. Hence

$$x+y=111011, \qquad x*y=110000, \qquad x'=001100$$

Then $\mathbf{B}^n$ is a Boolean algebra. Here $0=000\cdots0$ is the zero element, and $1=111\cdots1$ is the unit element. We note that $\mathbf{B}^n$ has 2^n elements.

(*c*) Let $\mathbf{D}_{70} = \{1, 2, 5, 7, 10, 14, 35, 70, \}$, the divisors of 70. Define $+$, $*$, and $'$ on $\mathbf{D}_{70}$ by

$$a + b = \text{lcm}\,(a, b), \qquad a * b = \gcd\,(a, b), \qquad a' = \frac{70}{a}$$

Then $\mathbf{D}_{70}$ is a Boolean algebra with 1 the zero element and 70 the unit element.

(*d*) Let $\mathcal{C}$ be a collection of sets closed under the set operations of union, intersection, and complement. Then $\mathcal{C}$ is a Boolean algebra with the empty set $\varnothing$ as the zero element and the universal set U as the unit element.

Subalgebras, Isomorphic Boolean Algebras

Suppose C is a nonempty subset of a Boolean algebra B. We say C is a *subalgebra* of B if C itself is a Boolean algebra (with respect to the operations of B). We note that C is a subalgebra of B if and only if C is closed under the three operations of B, i.e., $+$, $*$, and $'$. For example, $\{1, 2, 35, 70\}$ is a subalgebra of $\mathbf{D}_{70}$ in Example 15.1(c).

Two Boolean algebras B and B' are said to be *isomorphic* if there is a one-to-one correspondence $f: B \to B'$ which preserves the three operations, i.e., such that

$$f(a + b) = f(a) + f(b), \qquad f(a * b) = f(a) * f(b) \qquad \text{and} \qquad f(a') = f(a)'$$

for any elements, a, b in B.

15.3 DUALITY

The *dual* of any statement in a Boolean algebra B is the statement obtained by interchanging the operations $+$ and $*$, and interchanging their identity elements 0 and 1 in the original statement. For example, the dual of

$$(1 + a) * (b + 0) = b \qquad \text{is} \qquad (0 * a) + (b * 1) = b$$

Observe the symmetry in the axioms of a Boolean algebra B. That is, the dual of the set of axioms of B is the same as the original set of axioms. Accordingly, the important principle of duality holds in B. Namely,

Theorem 15.1 (Principle of Duality): The dual of any theorem in a Boolean algebra is also a theorem.

In other words, if any statement is a consequence of the axioms of a Boolean algebra, then the dual is also a consequence of those axioms since the dual statement can be proven by using the dual of each step of the proof of the original statement.

15.4 BASIC THEOREMS

Using the axioms $[\mathbf{B}_1]$ through $[\mathbf{B}_4]$, we prove (Problem 15.5) the following theorem.

Theorem 15.2: Let a, b, c be any elements in a Boolean algebra B.

(i) Idempotent laws:

(5*a*) $a + a = a$ (5*b*) $a * a = a$

(ii) Boundedness laws:

(6*a*) $a + 1 = 1$ (6*b*) $a * 0 = 0$

(iii) Absorption laws:

(7*a*) $a + (a * b) = a$ (7*b*) $a * (a + b) = a$

(iv) Associative laws

(8*a*) $(a + b) + c = a + (b + c)$ (8*b*) $(a * b) * c = a * (b * c)$

Theorem 15.2 and our axioms still do not contain all the properties of sets listed in Table 1-1. The next two theorems give us the remaining properties.

Theorem 15.3: Let a be any element of a Boolean algebra B.
(i) (Uniqueness of Complement) If $a + x = 1$ and $a * x = 0$, then $x = a'$.
(ii) (Involution law) $(a')' = a$.
(iii) $(9a)$ $0' = 1$. $(9b)$ $1' = 0$.

Theorem 15.4 (DeMorgan's laws): $(10a)$ $(a + b)' = a' * b'$. $(10b)$ $(a * b)' = a' + b'$.

We prove these theorems in Problems 15.6 and 15.7.

15.5 BOOLEAN ALGEBRAS AS LATTICES

By Theorem 15.2 and axiom $[\mathbf{B}_1]$, every Boolean algebra B satisfies the associative, commutative and absorption laws and hence is a lattice where $+$ and $*$ are the join and meet operations, respectively. With respect to this lattice, $a + 1 = 1$ implies $a \leq 1$ and $a * 0 = 0$ implies $0 \leq a$, for any element $a \in B$. Thus B is a bounded lattice. Furthermore, axioms $[\mathbf{B}_2]$ and $[\mathbf{B}_4]$ show that B is also distributive and complemented. Conversely, every bounded, distributive, and complemented lattice L satisfies the axioms $[\mathbf{B}_1]$ through $[\mathbf{B}_4]$. Accordingly, we have the following

Alternate Definition: A Boolean algebra B is a bounded, distributive and complemented lattice.

Since a Boolean algebra B is a lattice, it has a natural partial ordering (and so its diagram can be drawn). Recall (Chapter 14) that we define $a \leq b$ when the equivalent conditions $a + b = b$ and $a * b = a$ hold. Since we are in a Boolean algebra, we can actually say much more.

Theorem 15.5: The following are equivalent in a Boolean algebra:

$$(1)\quad a + b = b, \qquad (2)\quad a * b = a, \qquad (3)\quad a' + b = 1, \qquad (4)\quad a * b' = 0$$

Thus in a Boolean alegbra we can write $a \leq b$ whenever any of the above four conditions is known to be true.

EXAMPLE 15.2

(*a*) Consider a Boolean algebra of sets. Then set A precedes set B if A is a subset of B. Theorem 15.4 states that if $A \subseteq B$, as illustrated in the Venn diagram in Fig. 15-2, then the following conditions hold:

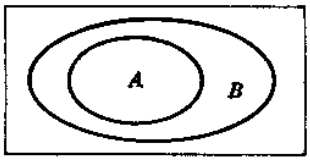
(1) $A \cup B = B$. (3) $A^c \cup B = U$.

(2) $A \cap B = A$. (4) $A \cap B^c = \varnothing$.

(*b*) Consider the Boolean $\mathbf{D}_{70}$. Then a precedes b if a divides b. In such a case, $\text{lcm}(a, b) = b$ and $\gcd(a, b) = a$. For example, let $a = 2$ and $b = 14$. Then the following conditions hold:

(1) $\text{lcm}(2, 14) = 14$. (3) $\text{lcm}(2', 14) = \text{lcm}(35, 14) = 70$.

(2) $\gcd(2, 14) = 2$. (4) $\gcd(2, 14') = \gcd(2, 5) = 1$.



A is a subset of *B*

Fig. 15-2

15.6 REPRESENTATION THEOREM

Let B be a finite Boolean algebra. Recall (Section 14.9) that an element a in B is an atom if a immediately succeeds 0, that is if $0 \ll a$. Let A be the set of atoms of B and let $P(A)$ be the Boolean algebra of all subsets of the set A of atoms. By Theorem 14.8, each $x \neq 0$ in B can be expressed uniquely (except for order) as the sum (join) of atoms, i.e., elements of A. Say,

$$x = a_1 + a_2 + \cdots + a_r$$

is such a representation. Consider the function $f: B \to P(A)$ defined by

$$f(x) = \{a_1, a_2, \ldots, a_r\}$$

The mapping is well defined since the representation is unique.

Theorem 15.6: The above mapping $f: B \to P(A)$ is an isomorphism.

Thus we see the intimate relationship between set theory and abstract Boolean algebras in the sense that every finite Boolean algebra is structurally the same as a Boolean algebra of sets.

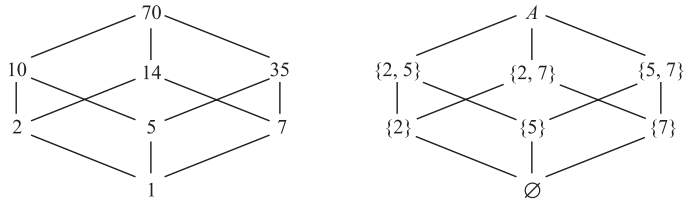
If a set A has n elements, then its power set $P(A)$ has 2^n elements. Thus the above theorem gives us our next result.

Corollary 15.7: A finite Boolean algebra has 2^n elements for some positive integer n.

EXAMPLE 15.3 Consider the Boolean algebra $\mathbf{D}_{70} = \{1, 2, 5, \ldots, 70\}$ whose diagram is given in Fig. 15-3(*a*). Note that $A = \{2, 5, 7\}$ is the set of atoms of $\mathbf{D}_{70}$. The following is the unique representation of each nonatom by atoms:

$$10 = 2 \vee 5, \qquad 14 = 2 \vee 7, \qquad 35 = 5 \vee 7, \qquad 70 = 2 \vee 5 \vee 7$$

Figure 15-3(*b*) gives the diagram of the Boolean algebra of the power set $P(A)$ of the set A of atoms. Observe that the two diagrams are structurally the same.



(*a*) $\mathbf{D}_{70}$ (*b*) $P(A)$

Fig. 15-3

15.7 SUM-OF-PRODUCTS FORM FOR SETS

This section motivates the concept of the sum-of-products form in Boolean algebra by an example of set theory. Consider the Venn diagram in Fig. 15-4 of three sets A, B, and C. Observe that these sets partition the rectangle (universal set) into eight numbered sets which can be represented as follows:

(1) $A \cap B \cap C$ (3) $A \cap B^c \cap C$ (5) $A \cap B^c \cap C^c$ (7) $A^c \cap B^c \cap C$

(2) $A \cap B \cap C^c$ (4) $A^c \cap B \cap C$ (6) $A^c \cap B \cap C^c$ (8) $A^c \cap B^c \cap C^c$

Each of these eight sets is of the form $A^* \cap B^* \cap C^*$ where:

$$A^* = A \text{ or } A^c, \qquad B^* = B \text{ or } B^c, \qquad C^* = C \text{ or } C^c$$

Consider any nonempty set expression E involving the sets A, B, and C, say,

$$E = [(A \cap B^c)^c \cup (A^c \cap C^c)] \cap [(B^c \cup C)^c \cap (A \cup C^c)]$$

Then E will represent some area in Fig. 15-4 and hence will uniquely equal the union of one or more of the eight sets.

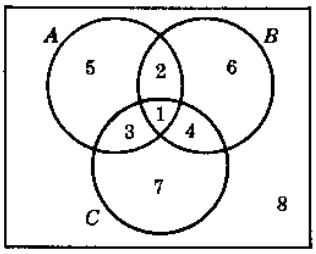


Fig. 15-4

Suppose we now interpret a union as a sum and an intersection as a product. Then the above eight sets are products, and the unique representation of E will be a sum (union) of products. This unique representation of E is the same as the complete sum-of-products expansion in Boolean algebras which we discuss below.

15.8 SUM-OF-PRODUCTS FORM FOR BOOLEAN ALGEBRAS

Consider a set of variables (or letters or symbols), say $x_1, x_2, \ldots, x_n$. A *Boolean expression* E in these variables, sometimes written $E(x_1, \ldots, x_n)$, is any variable or any expression built up from the variables using the Boolean operations $+$, $*$, and $'$. (Naturally, the expression E must be *well-formed*, that is, where $+$ and $*$ are used as binary operations, and $'$ is used as a unary operation.) For example,

$$E_1 = (x + y'z)' + (xyz' + x'y)' \qquad \text{and} \qquad E_2 = ((xy'z' + y)' + x'z)'$$

are Boolean expressions in x, y, and z.

A *literal* is a variable or complemented variable, such as x, x', y, y', and so on. A *fundamental product* is a literal or a product of two or more literals in which no two literals involve the same variable. Thus

$$xz', \quad xy'z, \quad x, \quad y', \quad x'yz.$$

are fundamental products, but $xyx'z$ and $xyzy$ are not. Note that any product of literals can be reduced to either 0 or a fundamental product, e.g., $xyx'z = 0$ since $xx' = 0$ (complement law), and $xyzy = xyz$ since $yy = y$ (idempotent law).

A fundamental product P_1 is said to be *contained in* (or *included in*) another fundamental product P_2 if the literals of P_1 are also literals of P_2. For example, $x'z$ is contained in $x'yz$, but $x'z$ is not contained in $xy'z$ since x' is not a literal of $xy'z$. Observe that if P_1 is contained in P_2, say $P_2 = P_1 * Q$, then, by the absorption law,

$$P_1 + P_2 = P_1 + P_1 * Q = P_1$$

Thus, for instance, $x'z + x'yz = x'z$.

Definition: A Boolean expression E is called a *sum-of-products* expression if E is a fundamental product or the sum of two or more fundamental products none of which is contained in another.

Definition: Let E be any Boolean expression. A *sum-of-products form* of E is an equivalent Boolean sum-of-products expression.

EXAMPLE 15.4 Consider the expressions

$$E_1 = xz' + y'z + xyz' \quad \text{and} \quad E_2 = xz' + x'yz' + xy'z$$

Although the first expression E_1 is a sum of products, it is not a sum-of-products expression. Specifically, the product xz' is contained in the product xyz'. However, by the absorption law, E_1 can be expressed as

$$E_1 = xz' + y'z + xyz' = xz' + xyz' + y'z = xz' + y'z$$

This yields a sum-of-products form for E_1. The second expression E_2 is already a sum-of-products expression.

Algorithm for Finding Sum-of-Products Forms

The following four-step algorithm uses the Boolean algebra laws to transform any Boolean expression E into an equivalent sum-of-products expression:

Algorithm 15.8A: The input is a Boolean expression E. The output is a sum-of-products expression equivalent to E.

Step 1. Use DeMorgan's laws and involution to move the complement operation into any parenthesis until finally the complement operation only applies to variables. Then E will consist only of sums and products of literals.

Step 2. Use the distributive operation to next transform E into a sum of products.

Step 3. Use the commutative, idempotent, and complement laws to transform each product in E into 0 or a fundamental product.

Step 4. Use the absorption and identity laws to finally transform E into a sum-of-products expression.

EXAMPLE 15.5 Suppose Algorithm 15.8A is applied to the following Boolean expression:

$$E = ((xy)'z)'((x' + z)(y' + z'))'$$

Step 1. Using DeMorgan's laws and involution, we obtain

$$E = (xy'' + z')((x' + z)' + (y' + z')') = (xy + z')(xz' + yz)$$

E now consists only of sums and products of literals

Step 2. Using the distributive laws, we obtain

$$E = xyxz' + xyyz + xz'z' + yzz'$$

E now is a sum of products.

Step 3. Using the commutative, idempotent, and complement laws, we obtain

$$E = xyz' + xyz + xz' + 0$$

Each term in E is a fundamental product or 0.

Step 4. The product ac' is contained in abc'; hence, by the absorption law,

$$xz' + (xz' * y) = xz'$$

Thus we may delete abc' from the sum. Also, by the identity law for 0, we may delete 0 from the sum. Accordingly,

$$E = xyz + xz'$$

E is now represented by a sum-of-products expression.

Complete Sum-of-Products Forms

A Boolean expression $E = E(x_1, x_2, \ldots, x_n)$ is said to be a *complete sum-of-products* expression if E is a sum-of-products expression where each product P involves all the n variables. Such a fundamental product P which involves all the variables is called a *minterm*, and there is a maximum of 2^n such products for n variables. The following theorem applies.

Theorem 15.8: Every nonzero Boolean expression $E = E(x_1, x_2, \ldots, x_n)$ is equivalent to a complete sum-of-products expression and such a representation is unique.

The above unique representation of E is called the *complete sum-of-products form* of E. Recall that Algorithm 15.8A tells us how to transform E into a sum-of-products form. The following algorithm shows how to transform a sum-of-products form into a complete sum-of-products form.

Algorithm 15.8B: The input is a Boolean sum-of-products expression $E = E(x_1, x_2, \ldots, x_n)$. The output is a complete sum-of-products expression equivalent to E.

Step 1. Find a product P in E which does not involve the variable x_i, and then multiply P by $x_i + x_i'$, deleting any repeated products. (This is possible since $x_i + x_i' = 1$, and $P + P = P$.)

Step 2. Repeat Step 1 until every product P in E is a minterm, i.e., every product P involves all the variables.

EXAMPLE 15.6 Express $E(x, y, z) = x(y'z)'$ in its complete sum-of-products form.

(*a*) Apply Algorithm 15.8A to E to obtain

$$E = x(y'z)' = x(y + z') = xy + xz'$$

Now E is represented by a sum-of-products expression.

(*b*) Apply Algorithm 15.8B to obtain

$$\begin{aligned} E &= xy(z + z') + xz'(y + y') = xyz + xyz' + xyz' + xy'z' \\ &= xyz + xyz' + xy'z' \end{aligned}$$

Now E is reprsented by its complete sum-of-products form.

Warning: The terminology in this section has not been standardized. The sum-of-products form for a Boolean expression E is also called the *disjunctive normal form* or DNF of E. The complete sum-of-products form for E is also called the *full disjunctive normal form*, or the *disjunctive canonical form*, or the *minterm canonical form* of E.

15.9 MINIMAL BOOLEAN EXPRESSIONS, PRIME IMPLICANTS

There are many ways of representing the same Boolean expression E. Here we define and investigate a minimal sum-of-products form for E. We must also define and investigate prime implicants of E since

the minimal sum-of-products involves such prime implicants. Other minimal forms exist, but their investigation lies beyond the scope of this text.

Minimal Sum-of-Products

Consider a Boolean sum-of-products expression E. Let E_L denote the number of literals in E (counted according to multiplicity), and let E_S denote the number of summands in E. For instance, suppose

$$E = xyz' + x'y't + xy'z't + x'yzt$$

Then $E_L = 3 + 3 + 4 + 4 = 14$ and $E_S = 4$.

Suppose E and F are equivalent Boolean sum-of-products expressions. We say E is *simpler* than F if:

$$\text{(i)} \quad E_L < F_L \text{ and } E_S \leq F_L, \qquad \text{or} \qquad \text{(ii)} \quad E_L \leq F_L \text{ and } E_S < F_L$$

We say E is *minimal* if there is no equivalent sum-of-products expression which is simpler than E. We note that there can be more than one equivalent minimal sum-of-products expressions.

Prime Implicants

A fundamental product P is called a *prime implicant* of a Boolean expression E if

$$P + E = E$$

but no other fundamental product contained in P has this property. For instance, suppose

$$E = xy' + xyz' + x'yz'$$

One can show (Problem 15.15) that:

$$xz' + E = E \qquad \text{but} \qquad x + E \neq E \qquad \text{and} \qquad z' + E \neq E$$

Thus xz' is a prime implicant of E.

The following theorem applies.

Theorem 15.9: A minimal sum-of-products form for a Boolean expression E is a sum of prime implicants of E.

The following subsections give a method for finding the prime implicants of E based on the notion of the consensus of fundamental products. This method can then be used to find a minimal sum-of-products form for E. Section 15.12 gives a geometric method for finding such prime implicants.

Consensus of Fundamental Products

Let P_1 and P_2 be fundamental products such that exactly one variable, say x_k, appears uncomplemented in one of P_1 and P_2 and complemented in the other. Then the *consensus* of P_1 and P_2 is the product (without repetitions) of the literals of P_1 and the literals of P_2 after x_k and x_k' are deleted. (We do not define the consensus of $P_1 = x$ and $P_2 = x'$.)

The following lemma (proved in Problem 15.19) applies.

Lemma 15.10: Suppose Q is the consensus of P_1 and P_2. Then $P_1 + P_2 + Q = P_1 + P_2$.

EXAMPLE 15.7 Find the consensus Q of P_1 and P_2 where:

(*a*) $P_1 = xyz's$ and $P_2 = xy't$.
Delete y and y' and then multiply the literals of P_1 and P_2 (without repetition) to obtain $Q = xz'st$.

(*b*) $P_1 = xy'$ and $P_2 = y$.
Deleting y and y' yields $Q = x$.

(*c*) $P_1 = x'yz$ and $P_2 = x'yt$.
No variable appears uncomplemented in one of the products and complemented in the other. Hence P_1 and P_2 have no consensus.

(*d*) $P_1 = x'yz$ and $P_2 = xyz'$.
Each of x and z appear complemented in one of the products and uncomplemented in the other. Hence P_1 and P_2 have no consensus.

Consensus Method for Finding Prime Implicants

The following algorithm, called the *consensus method*, is used to find the prime implicants of a Boolean expression.

Algorithm 15.9A (Consensus Method): The input is a Boolean expression $E = P_1 + P_2 + \cdots + P_m$ where the Ps are fundamental products. The output expresses E as a sum of its prime implicants (Theorem 15.11).

Step 1. Delete any fundamental product P_i which includes any other fundamental product P_j. (Permissible by the absorption law.)

Step 2. Add the consensus of any P_i and P_j providing Q does not include any of the Ps. (Permissible by Lemma 15.10.)

Step 3. Repeat Step 1 and/or Step 2 until neither can be applied.

The following theorem gives the basic property of the above algorithm.

Theorem 15.11: The consensus method will eventually stop, and then E will be the sum of its prime implicants.

EXAMPLE 15.8 Let $E = xyz + x'z' + xyz' + x'y'z + x'yz'$. Then:

$$\begin{aligned}
E &= xyz + x'z' + xyz' + x'y'z && (x'yz' \text{ includes } x'z') \\
&= xyz + x'y' + xyz' + x'y'z + xy && (\text{consensus of } xyz \text{ and } xyz') \\
&= x'z' + x'y'z + xy && (xyz \text{ and } xyz' \text{ include } xy) \\
&= x'z' + x'y'z + xy + x'y' && (\text{consensus of } x'z' \text{ and } x'y'z) \\
&= x'z' + xy + x'y' && (x'y'z \text{ includes } x'y') \\
&= x'z' + xy + x'y' + yz' && (\text{consensus of } x'z' \text{ and } xy)
\end{aligned}$$

Now neither step in the consensus method will change E. Thus E is the sum of its prime implicants, which appear in the last line, that is, $x'z'$, xy, $x'y'$, and yz'.

Finding a Minimal Sum-of-Products Form

The consensus method (Algorithm 15.9A) can be used to express a Boolean expression E as a sum of all its prime implicants. Using such a sum, one may find a minimal sum-of-products form for E as follows.

Algorithm 15.9B: The input is a Boolean expression $E = P_1 + P_2 + \cdots + P_m$ where the Ps are all the prime implicants of E. The output expresses E as a minimal sum-of-products.

Step 1. Express each prime implicant P as a complete sum-of-products.

Step 2. Delete one by one those prime implicants whose summands appear among the summands of the remaining prime implicants.

EXAMPLE 15.9 We apply Algorithm 15.9B to

$$E = x'z' + xy + x'y' + yz'$$

(By Example 15.8, E is now expressed as the sum of all its prime implicants.)

Step 1. Express each prime implicant of E as a complete sum-of-products to obtain:

$$\begin{aligned} x'z' &= x'z'(y + y') = x'yz' + x'y'z' \\ xy &= xy(z + z') = xyz + xyz' \\ x'y' &= x'y'(z + z') = x'y'z + x'y'z' \\ yz' &= yz'(x + x') = xyz' + x'yz' \end{aligned}$$

Step 2. The summands of $x'z'$ are $x'yz$ and $x'y'z'$ which appear among the other summands. Thus delete $x'z'$ to obtain

$$E = xy + x'y' + yz'$$

The summands of no other prime implicant appear among the summands of the remaining prime implicants, and hence this is a minimal sum-of-products form for E. In other words, none of the remaining prime implicants is *superfluous*, that is, none can be deleted without changing E.

15.10 LOGIC GATES AND CIRCUITS

Logic circuits (also called *logic networks*) are structures which are built up from certain elementary circuits called *logic gates*. Each logic circuit may be viewed as a machine L which contains one or more input devices and exactly one output device. Each input device in L sends a signal, specifically, a *bit* (binary digit),

$$0 \quad \text{or} \quad 1$$

to the circuit L, and L processes the set of bits to yield an output bit. Accordingly, an n-bit sequence may be assigned to each input device, and L processes the input sequences one bit at a time to produce an n-bit output sequence. First we define the logic gates, and then we investigate the logic circuits.

Logic Gates

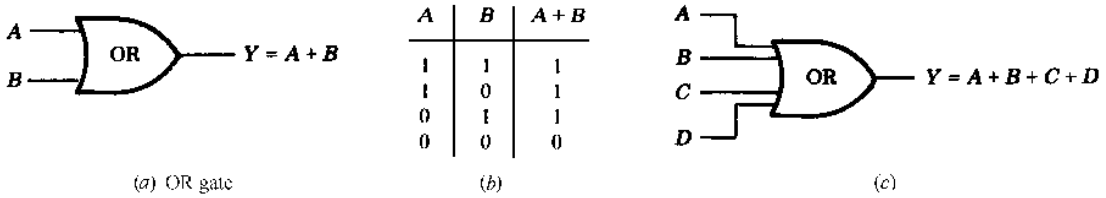
There are three basic logic gates which are described below. We adopt the convention that the lines entering the gate symbol from the left are input lines and the single line on the right is the output line.

(*a*) ***OR Gate***: Figure 15-5(*a*) shows an OR gate with inputs A and B and output $Y = A + B$ where "addition" is defined by the "truth table" in Fig. 15-5(*b*). Thus the output $Y = 0$ only when inputs $A = 0$ and $B = 0$. Such an OR gate may have more than two inputs. Figure 15-5(*c*) shows an OR gate with four inputs, A, B, C, D, and output $Y = A + B + C + D$. The output $Y = 0$ if and only if all the inputs are 0.

Suppose, for instance, the input data for the OR gate in Fig. 15-15(*c*) are the following 8-bit sequences:

$$A = 10000101, \qquad B = 10100001, \qquad C = 00100100, \qquad D = 10010101$$

The OR gate only yields 0 when all input bits are 0. This occurs only in the 2nd, 5th, and 7th positions (reading from left to right). Thus the output is the sequence $Y = 10110101$.



(*a*) OR gate (*b*) (*c*)

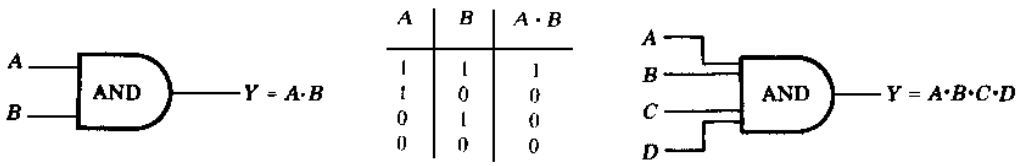
Fig. 15-5

(*b*) ***AND Gate***: Figure 15-6(*a*) shows an AND gate with inputs A and B and output $Y = A \cdot B$ (or simply $Y = AB$) where "multiplication" is defined by the "truth table" in Fig. 15-6(*b*). Thus the output $Y = 1$ when inputs $A = 1$ and $B = 1$; otherwise $Y = 0$. Such an AND gate may have more than two inputs. Figure 15-6(*c*) shows an AND gate with four inputs, A, B, C, D, and output $Y = A \cdot B \cdot C \cdot D$. The output $Y = 1$ if and only if all the inputs are 1.

Suppose, for instance, the input data for the AND gate in Fig. 15-6(*c*) are the following 8-bit sequences:

$$A = 11100111, \qquad B = 01111011, \qquad C = 01110011, \qquad D = 11101110$$

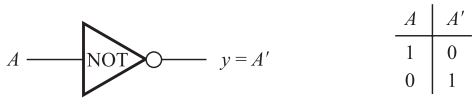
The AND gate only yields 1 when all input bits are 1. This occurs only in the 2nd, 3rd, and 7th positions. Thus the output is the sequence $Y = 01100010$.



(*a*) AND gate (*b*) (*c*)

Fig. 15-6

(*c*) ***NOT Gate***: Figure 15-7(*a*) shows a NOT gate, also called an *inverter*, with input A and output $Y = A'$ where "inversion", denoted by the prime, is defined by the "truth table" in Fig. 15-7(*b*). The value of the output $Y = A'$ is the opposite of the input A; that is, $A' = 1$ when $A = 0$ and $A' = 0$ when $A = 1$. We emphasize that a NOT gate can have only one input, whereas the OR and AND gates may have two or more inputs.



(*a*) NOT gate (*b*)

Fig. 15-7

Suppose, for instance, a NOT gate is asked to process the following three sequences:

$$A_1 = 110001, \qquad A_2 = 10001111, \qquad A_3 = 101100111000$$

The NOT gate changes 0 to 1 and 1 to 0. Thus

$$A_1' = 001110, \qquad A_2' = 01110000, \qquad A_3' = 010011000111$$

are the three corresponding outputs.

Logic Circuits

A logic circuit L is a well-formed structure whose elementary components are the above OR, AND, and NOT gates. Figure 15-8 is an example of a logic circuit with inputs A, B, C and output Y. A dot indicates a place where the input line splits so that its bit signal is sent in more than one direction. (Frequently, for notational convenience, we may omit the word from the interior of the gate symbol.) Working from left to right, we express Y in terms of the inputs A, B, C as follows. The output of the AND gate is $A \cdot B$, which is then negated to yield $(A \cdot B)'$. The output of the lower OR gate is $A' + C$, which is then negated to yield $(A' + C)'$. The output of the OR gate on the right, with inputs $(A \cdot B)'$ and $(A' + C)'$, gives us our desired representation, that is,

$$Y = (A \cdot B)' + (A' + C)'$$

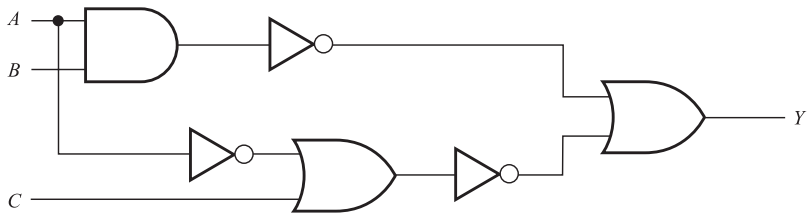


Fig. 15-8

Logic Circuits as a Boolean Algebra

Observe that the truth tables for the OR, AND, and NOT gates are respectively identical to the truth tables for the propositions $p \vee q$ (disjunction, "p or q"), $p \wedge q$ (conjunction, "p and q"), and $\neg p$ (negation, "not p"), which appear in Section 4.3. The only difference is that 1 and 0 are used instead of T and F. Thus the logic circuits satisfy the same laws as do propositions and hence they form a Boolean algebra. We state this result formally.

Theorem 15.12: Logic circuits form a Boolean Algebra.

Accordingly, all terms used with Boolean algebras, such as, complements, literals, fundamental products, minterms, sum-of-products, and complete sum-of-products, may also be used with our logic circuits.

AND-OR Circuits

The logic circuit L which corresponds to a Boolean sum-of-products expression is called an AND-OR circuit. Such a circuit L has several inputs, where:

(1) Some of the inputs or their complements are fed into each AND gate.
(2) The outputs of all the AND gates are fed into a single OR gate.
(3) The output of the OR gate is the output for the circuit L.

The following illustrates this type of a logic circuit.

EXAMPLE 15.10 Figure 15-9 is a typical AND-OR circuit with three inputs A, B, C and output Y. We can easily express Y as a Boolean expression in the inputs A, B, C as follows. First we find the output of each AND gate:

(a) The inputs of the first AND gate are A, B, C; hence $A \cdot B \cdot C$ is the output.

(b) The inputs of the second AND gate are A, B', C; hence $A \cdot B' \cdot C$ is the output.

(c) The inputs of the third AND gate are A' and B; hence $A' \cdot B$ is the output.

Then the sum of the outputs of the AND gates is the output of the OR gate, which is the output Y of the circuit. Thus:

$$Y = A \cdot B \cdot C + A \cdot B' \cdot C + A' \cdot B$$

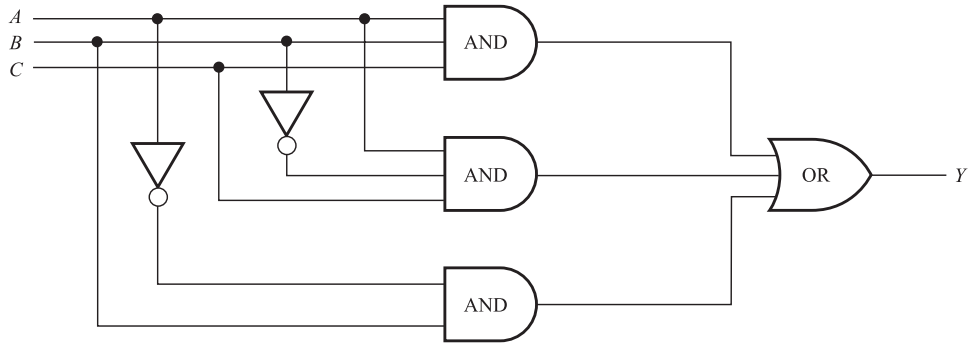


Fig. 15-9

NAND and NOR Gates

There are two additional gates which are equivalent to combinations of the above basic gates.

(a) A NAND gate, pictured in Fig. 15-10(a), is equivalent to an AND gate followed by a NOT gate.
(b) A NOR gate, pictured in Fig. 15-10(b), is equivalent to an OR gate followed by a NOT gate.

The truth tables for these gates (using two inputs A and B) appear in Fig. 15-10(c). The NAND and NOR gates can actually have two or more inputs just like the corresponding AND and OR gates. Furthermore, the output of a NAND gate is 0 if and only if all the inputs are 1, and the output of a NOR gate is 1 if and only if all the inputs are 0.

(a) NAND gate

(b) NOR gate

A	B	NAND	NOR
1	1	0	0
1	0	1	0
0	1	1	0
0	0	1	1

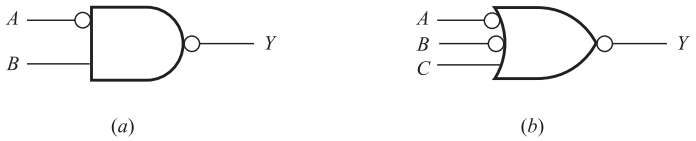
(c)

Fig. 15-10

Observe that the only difference between the AND and NAND gates and between the OR and NOR gates is that the NAND and NOR gates are each followed by a circle. Some texts also use such a small

circle to indicate a complement before a gate. For example, the Boolean expressions corresponding to the two logic circuits in Fig. 15-11 are as follows:

$$(a) \quad Y = (A'B)', \qquad (b) \quad Y = (A' + B' + C)'$$



(a) (b)

Fig. 15-11

15.11 TRUTH TABLES, BOOLEAN FUNCTIONS

Consider a logic circuit L with $n = 3$ input devices A, B, C and output Y, say

$$Y = A \cdot B \cdot C + A \cdot B' \cdot C + A' \cdot B$$

Each assignment of a set of three bits to the inputs A, B, C yields an output bit for Y. All together there are $2^n = 2^3 = 8$ possible ways to assign bits to the inputs as follows:

$$000, \quad 001, \quad 010, \quad 011, \quad 100, \quad 101, \quad 110, \quad 111$$

The assumption is that the sequence of first bits is assigned to A, the sequence of second bits to B, and the sequence of third bits to C. Thus the above set of inputs may be rewritten in the form

$$A = 00001111, \qquad B = 00110011, \qquad C = 01010101$$

We emphasize that these three $2^n = 8$-bit sequences contain the eight possible combinations of the input bits.

The *truth table* $T = T(L)$ of the above circuit L consists of the output sequence Y that corresponds to the input sequences A, B, C. This truth table T may be expressed using fractional or relational notation, that is, T may be written in the form

$$T(A, B, C) = Y \qquad \text{or} \qquad T(L) = [A, B, C; Y]$$

This form for the truth table for L is essentially the same as the truth table for a proposition discussed in Section 4.4. The only difference is that here the values for A, B, C, and Y are written horizontally, whereas in Section 4.4 they are written vertically.

Consider a logic circuit L with n input devices. There are many ways to form n input sequences $A_1, A_2, \ldots, A_n$ so that they contain the 2^n different possible combinations of the input bits. (Note that each sequence must contain 2^n bits.) One assignment scheme is as follows:

$\mathbf{A}_1$: Assign 2^{n-1} bits which are 0s followed by 2^{n-1} bits which are 1s.
$\mathbf{A}_2$: Repeatedly assign 2^{n-2} bits which are 0s followed by 2^{n-2} bits which are 1s.
$\mathbf{A}_3$: Repeatedly assign 2^{n-3} bits which are 0s followed by 2^{n-3} bits which are 1s.

And so on. The sequences obtained in this way will be called *special sequences*. Replacing 0 by 1 and 1 by 0 in the special sequences yields the complements of the special sequences.

Remark: Assuming the input are the special sequences, we frequently do not need to distinguish between the truth table

$$T(L) = [A_1, A_2, \ldots, A_n; Y]$$

and the output Y itself.

EXAMPLE 15.11

(*a*) Suppose a logic circuit L has $n = 4$ inputs devices A, B, C, D. The $2^n = 2^4 = 16$-bit special sequences for A, B, C, D follow:

$$A = 0000000011111111, \qquad C = 0011001100110011$$
$$B = 0000111100001111, \qquad D = 0101010101010101$$

That is:

(1) A begins with eight 0s followed by eight 1s. (Here $2^{n-1} = 2^3 = 8$.)
(2) B begins with four 0s followed by four 1s, and so on. (Here $2^{n-2} = 2^2 = 4$.)
(3) C begins with two 0s followed by two 1s, and so on. (Here $2^{n-3} = 2^1 = 2$.)
(4) D begins with one 0 followed by one 1, and so on. (Here $2^{n-4} = 2^0 = 1$.)

(*b*) Suppose a logic circuit L has $n = 3$ inputs devices A, B, C. The $2^n = 2^3 = 8$-bit special sequences for A, B, C and their complements A', B', C' are as follows:

$$A = 00001111, \qquad B = 00110011, \qquad C = 01010101$$
$$A' = 11110000, \qquad B' = 11001100, \qquad C' = 10101010$$

The following is a three-step algorithm for finding the truth table for a logic circuit L where the output Y is given by a Boolean sum-of-products expression in the inputs.

Algorithm 15.11: The input is a Boolean sum-of-products expression $Y = Y(A_1, A_2, \ldots)$.
Step 1. Write down the special sequences for the inputs $A_1, A_2, \ldots$ and their complements.
Step 2. Find each product appearing in Y. (Recall that a product $X_1 \cdot X_2 \cdots = 1$ in a position if and only if all the $X_1, X_2, \ldots$ have 1 in the position.)
Step 3. Find the sum Y of the products. (Recall that a sum $X_1 + X_2 + \cdots = 0$ in a position if and only if all the $X_1, X_2, \ldots$ have 0 in the position.)

EXAMPLE 15.12 Algorithm 15.11 is used to find the truth table $T = T(L)$ of the logic circuit L in Fig. 15.9 or, equivalently, of the above Boolean sum-of-products expression

$$Y = A \cdot B \cdot C + A \cdot B' \cdot C + A' \cdot B$$

(1) The special sequences and their complements appear in Example 15.11(*b*).
(2) The products are as follows:

$$A \cdot B \cdot C = 00000001, \qquad A \cdot B' \cdot C = 00000100, \qquad A' \cdot B = 00110000$$

(3) The sum is $Y = 00110101$.

Accordingly,

$$T(00001111,\ 00110011,\ 01010101) = 00110101$$

or simply $T(L) = 00110101$ where we assume the input consists of the special sequences.

Boolean Functions

Let E be a Boolean expression with n variables $x_1, x_2, \ldots, x_n$. The entire discussion above can also be applied to E where now the special sequences are assigned to the variables $x_1, x_2, \ldots, x_n$ instead of the input devices $A_1, A_2, \ldots, A_n$. The truth table $T = T(E)$ of E is defined in the same way as the truth table $T = T(L)$ for a logic circuit L. For example, the Boolean expression

$$E = xyz + xy'z + x'y$$

which is analogous to the logic circuit L in Example 15.12, yields the truth table

$$T(00001111,\ 00110011,\ 01010101) = 00110101$$

or simply $T(E) = 00110101$, where we assume the input consists of the special sequences.

Remark: The truth table for a Boolean expression $E = E(x_1, x_2, \ldots, x_n)$ with n variables may also be viewed as a "Boolean" function from B^n into B. [The Boolean algebras B^n and $B = \{0, 1\}$ are defined in Example 15.1] That is, each element in B^n is a list of n bits which when assigned to the list of variables in E produces an element in B. The truth table $T(E)$ of E is simply the graph of the function.

EXAMPLE 15.13

(*a*) Consider Boolean expressions $E = E(x, y, z)$ with three variables. The eight minterms (fundamental products involving all three variables) are as follows:

$$xyz, \quad xyz', \quad xy'z, \quad x'yz, \quad xy'z', \quad x'yz', \quad x'y'z'$$

The truth tables for these minterms (using the special sequences for x, y, z) follow:

$$xyz = 00000001, \quad xyz' = 00000010, \quad xy'z = 00000100, \quad x'yz = 00001000$$
$$xy'z' = 00010000, \quad x'yz' = 00100000, \quad x'y'z = 01000000, \quad x'y'z' = 10000000$$

Observe that each minterm assumes the value 1 in only one of the eight positions.

(*b*) Consider the Boolean expression $E = xyz' + x'yz + x'y'z$. Note that E is a complete sum-of-products expression containing three minterms. Accordingly, the truth table $T = T(E)$ for E, using the special sequences for x, y, z, can be easily obtained from the sequences in part (*a*). Specifically, the truth table $T(E)$ will contain exactly three 1s in the same positions as the 1s in the three minterms in E. Thus

$$T(00001111, \ 00110011, \ 01010101) = 01001010$$

or simply $T(E) = 01001010$.

15.12 KARNAUGH MAPS

Karnaugh maps, where minterms involving the same variables are represented by squares, are pictorial devices for finding prime implicants and minimal forms for Boolean expressions involving at most six variables. We will only treat the cases of two, three, and four variables. In the context of Karnaugh maps, we will sometimes use the terms "squares" and "minterm" interchangeably. Recall that a minterm is a fundamental product which involves all the variables, and that a complete sum-of-products expression is a sum of minterms.

First we need to define the notion of adjacent products. Two fundamental products P_1 and P_2 are said to be *adjacent* if P_1 and P_2 have the same variables and if they differ in exactly one literal. Thus there must be an uncomplemented variable in one product and complemented in the other. In particular, the sum of two such adjacent products will be a fundamental product with one less literal.

EXAMPLE 15.14 Find the sum of adjacent products P_1 and P_2 where:

(*a*) $P = xyz'$ and $P_2 = xy'z'$.

$$P_1 + P_2 = xyz' + xy'z' = xz'(y + y') = xz'(1) = xz'$$

(*b*) $P_1 = x'yzt$ and $P_2 = x'yz't$.

$$P_1 + P_2 = x'yzt + x'yz't = x'yt(z + z') = x'yt(1) = x'yt$$

(*c*) $P_1 = x'yzt$ and $P_2 = xyz't$.

Here P_1 and P_2 are not adjacent since they differ in two literals. In particular,

$$P_1 + P_2 = x'yzt + xyz't = (x' + x)y(z + z')t = (1)y(1)t = yt$$

(*d*) $P_1 = xyz'$ and $P_2 = xyzt$.

Here P_1 and P_2 are not adjacent since they have different variables. Thus, in particular, they will not appear as squares in the same Karnaugh map.

Case of Two Variables

The Karnaugh map corresponding to Boolean expressions $E = E(x, y)$ with two variables x and y is shown in Fig. 15-12(a). The Karnaugh map may be viewed as a Venn diagram where x is represented by the points in the upper half of the map, shaded in Fig. 15-12(b), and y is represented by the points in the left half of the map, shaded in Fig. 15-12(c). Thus x' is represented by the points in the lower half of the map, and y' is represented by the points in the right half of the map. Accordingly, the four possible minterms with two literals,

$$xy, \quad xy', \quad x'y, \quad x'y'$$

are represented by the four squares in the map, as labeled in Fig. 15-12(d). Note that two such squares are adjacent, as defined above, if and only if the squares are geometrically adjacent (have a side in common).

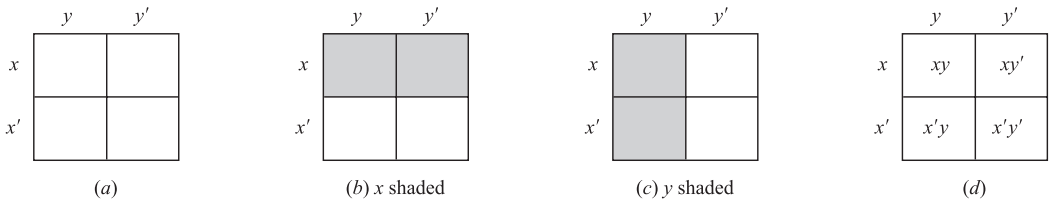


Fig. 15-12

Any complete sum-of-products Boolean expression $E(x, y)$ is a sum of minterms and hence can be represented in the Karnaugh map by placing checks in the appropriate squares. A prime implicant of $E(x, y)$ will be either a pair of adjacent squares in E or an *isolated* square, i.e., a square which is not adjacent to any other square of $E(x, y)$. A minimal sum-of-products form for $E(x, y)$ will consist of a minimal number of prime implicants which cover all the squares of $E(x, y)$ as illustrated in the next example.

EXAMPLE 15.15 Find the prime implicants and a minimal sum-of-products form for each of the following complete sum-of-products Boolean expressions:

$$(a) \ E_1 = xy + xy'; \quad (b) \quad E_2 = xy + x'y + x'y'; \quad (c) \quad E_3 = xy + x'y'$$

This can be solved by using Karnaugh maps as follows:

(a) Check the squares corresponding to xy and xy' as in Fig. 15-13(a). Note that E_1 consists of one prime implicant, the two adjacent squares designated by the loop in Fig. 15-13(a). This pair of adjacent squares represents the variable x, so x is a (the only) prime implicant of E_1. Consequently, $E_1 = x$ is its minimal sum.

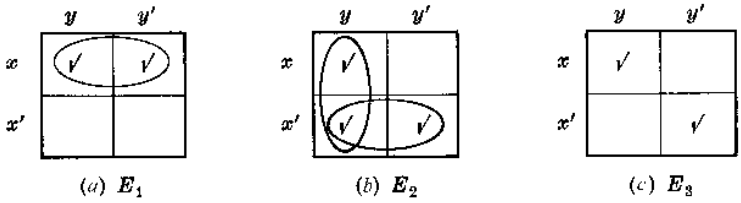


Fig. 15-13

(*b*) Check the squares corresponding to xy, $x'y$, and $x'y'$ as in Fig. 15-13(*b*). Note that E_2 contains two pairs of adjacent squares (designated by the two loops) which include all the squares of E_2. The vertical pair represents y and the horizontal pair represents x'; hence y and x' are the prime implicants of E_2. Thus $E_2 = x' + y$ is its minimal sum.

(*c*) Check the squares corresponding to xy and $x'y'$ as in Fig. 15-13(*c*). Note that E_3 consists of two isolated squares which represent xy and $x'y'$; hence xy and $x'y'$ are the prime implicants of E_3 and $E_3 = xy + x'y'$ is its minimal sum.

Case of Three Variables

The Karnaugh map corresponding to Boolean expressions $E = E(x, y, z)$ with three variables x, y, z is shown in Fig. 15-14(*a*). Recall that there are exactly eight minterms with three variable:

$$xyz, \quad xyz', \quad xy'z', \quad xy'z, \quad x'yz, \quad x'yz', \quad x'y'z', \quad x'y'z$$

These minterms are listed so that they correspond to the eight squares in the Karnaugh map in the obvious way.

Furthermore, in order that every pair of adjacent products in Fig. 15.14(*a*) are geometrically adjacent, the right and left edges of the map must be identified. This is equivalent to cutting out, bending, and gluing the map along the identified edges to obtain the cylinder pictured in Fig. 15-14(*b*) where adjacent products are now represented by squares with one edge in common.

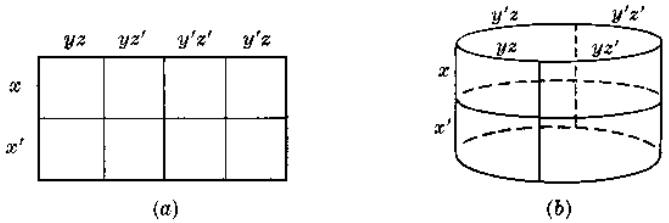


Fig. 15-14

Viewing the Karnaugh map in Fig. 15-14(*a*) as a Venn diagram, the areas represented by the variables x, y, and z are shown in Fig. 15-15. Specifically, the variable x is still represented by the points in the upper half of the map, as shaded in Fig. 15-15(*a*), and the variable y is still represented by the points in the left half of the map, as shaded in Fig. 15-15(*b*). The new variable z is represented by the points in the left and right quarters of the map, as shaded in Fig. 15-15(*c*). Thus x', y', and z' are represented, respectively, by points in the lower half, right half, and middle two quarters of the map.

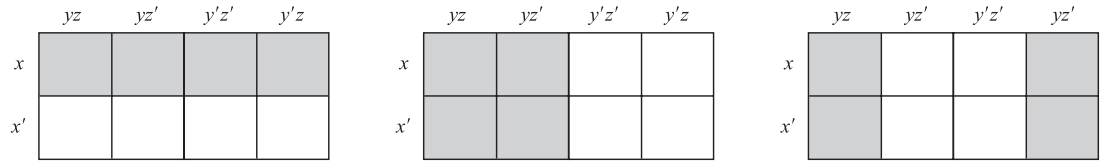


Fig. 15-15

By a *basic rectangle* in the Karnaugh map with three variables, we mean a square, two adjacent squares, or four squares which form a one-by-four or a two-by-two rectangle. These basic rectangles correspond to fundamental products of three, two, and one literal, respectively. Moreover, the

fundamental product represented by a basic rectangle is the product of just those literals that appear in every square of the rectangle.

Suppose a complete sum-of-products Boolean expression $E = E(x, y, z)$ is represented in the Karnaugh map by placing checks in the appropriate squares. A prime implicant of E will be a *maximal basic rectangle* of E, i.e., a basic rectangle contained in E which is not contained in any larger basic rectangle in E. A minimal sum-of-products form for E will consist of a *minimal cover* of E, that is, a minimal number of maximal basic rectangles of E which together include all the squares of E.

EXAMPLE 15.16 Find the prime implicants and a minimal sum-of-products form for each of the following complete sum-of-products Boolean expressions:

(*a*) $E_1 = xyz + xyz' + x'yz' + x'y'z$.

(*b*) $E_2 = xyz + xyz' + xy'z + x'yz + x'y'z$.

(*c*) $E_3 = xyz + xyz' + x'yz' + x'y'z' + x'y'z$.

This can be solved by using Karnaugh maps as follows:

(*a*) Check the squares corresponding to the four summands as in Fig. 15-16(*a*). Observe that E_1 has three prime implicants (maximal basic rectangles), which are circled; these are xy, yz', and $x'y'z$. All three are needed to cover E_1; hence the minimal sum for E_1 is

$$E_1 = xy + yz' + x'y'z$$

(*b*) Check the squares corresponding to the five summands as in Fig. 15-16(*b*). Note that E_2 has two prime implicants, which are circled. One is the two adjacent squares which represents xy, and the other is the two-by-two square (spanning the identified edges) which represents z. Both are needed to cover E_2, so the minimal sum for E_2 is

$$E_2 = xy + z$$

(*c*) Check the squares corresponding to the five summands as in Fig. 15-16(*c*). As indicated by the loops, E_3 has four prime implicants, xy, yz', $x'z'$, and $x'y'$. However, only one of the two dashed ones, i.e., one of yz' or $x'z'$, is needed in a minimal cover of E_3. Thus E_3 has two minimal sums:

$$E_3 = xy + yz' + x'y' = xy + x'z' + x'y'$$

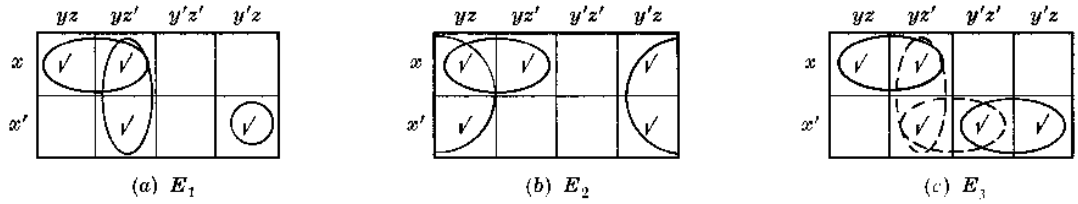


Fig. 15-16

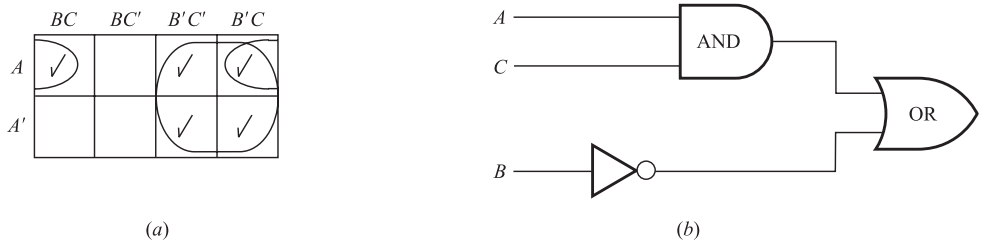
EXAMPLE 15.17 Design a three-input minimal AND-OR circuit L with the following truth table:

$$T = [A, B, C; L] = [00001111,\ 00110011,\ 01010101;\ 11001101]$$

From the truth table we can read off the complete sum-of-products form for L (as in Example 15.10):

$$L = A'B'C' + A'B'C + AB'C' + AB'C + ABC$$

The associated Karnaugh map is shown in Fig. 15-17(*a*). Observe that L has two prime implicants, B' and AC, in its minimal cover; hence $L = B' + AC$ is a minimal sum for L. Figure 15-17(*b*) gives the corresponding minimal AND-OR circuit for L.



(*a*) (*b*)

Fig. 15-17

Case of Four Variables

The Karnaugh map corresponding to Boolean expressions $E = E(x, y, z, t)$ with four variables x, y, z, t is shown in Fig. 15-18. Each of the 16 squares corresponds to one of the 16 minterms with four variables,

$$xyzt, \quad xyzt', \quad xyz't', \quad xyz't, \quad \ldots, x'yz't$$

as indicated by the labels of the row and column of the square. Observe that the top line and the left side are labeled so that adjacent products differ in precisely one literal. Again we must identify the left edge with the right edge (as we did with three variables) but we must also identify the top edge with the bottom edge. (These identifications give rise to a donut-shaped surface called a *torus*, and we may view our map as really being a torus.)

A *basic rectangle* in a four-variable Karnaugh map is a square, two adjacent squares, four squares which form a one-by-four or two-by-two rectangle, or eight squares which form a two-by-four rectangle. These rectangles correspond to fundamental products with four, three, two, and one literal, respectively. Again, maximal basic rectangles are the prime implicants. The minimization technique for a Boolean expression $E(x, y, z, t)$ is the same as before.

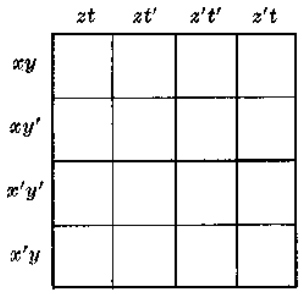


Fig. 15-18

EXAMPLE 15.18 Find the fundamental product P represented by the basic rectangle in the Karnaugh maps shown in Fig. 15-19.

In each case, find the literals which appear in all the squares of the basic rectangle; P is the product of such literals.

(*a*) x y, and z' appear in both squares; hence $P = xy'z'$.

(*b*) Only y and z appear in all four squares; hence $P = yz$.

(*c*) Only t appears in all eight squares; hence $P = t$.

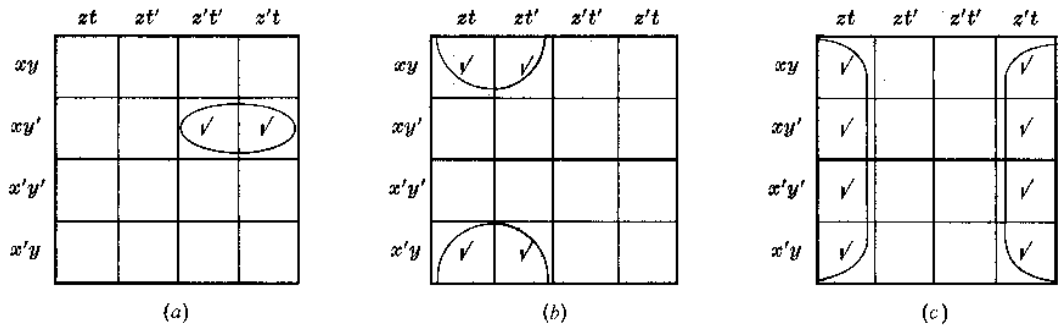


Fig. 15-19

EXAMPLE 15.19 Use a Karnaugh map to find a minimal sum-of-products form for

$$E = xy' + xyz + x'y'z' + x'yzt'$$

Check all the squares representing each fundamental product. That is, check all four squares representing xy', the two squares representing xyz, the two squares representing $x'y'z'$, and the one square representing $x'yzt'$, as in Fig. 15-20. A minimal cover of the map consists of the three designated maximal basic rectangles. The two-by-two squares represent the fundamental products xz and $y'z'$, and the two adjacent squares (on top and bottom) represents yzt'. Hence

$$E = xz + y'z' + yzt'$$

is a minimal sum for E.

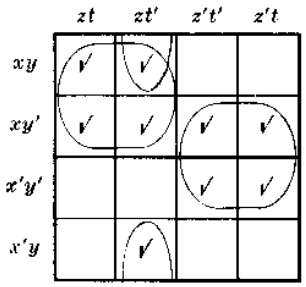


Fig. 15-20

Solved Problems

BOOLEAN ALGEBRAS

15.1. Write the dual of each Boolean equation: (*a*) $(a * 1) * (0 + a') = 0$; (*b*) $a + a'b = a + b$.

(*a*) To obtain the dual equation, interchange $+$ and $*$, and interchange 0 and 1. Thus

$$(a + 0) + (1 * a') = 1$$

(*b*) First write the equation using $*$ to obtain $a + (a' * b) = a + b$. Then the dual is $a * (a' + b) = a * b$, which can be written as

$$a(a' + b) = ab$$

15.2. Recall (Chapter 14), that the set $\mathbf{D}_m$ of divisors of m is a bounded, distributive lattice with $a + b = a \vee b = \text{lcm}(a, b)$ and $a * b = a \wedge b = \gcd(a, b)$. (*a*) Show that $\mathbf{D}_m$ is a Boolean algebra if m is square free, i.e., if m is a product of distinct primes. (*b*) Find the atoms of $\mathbf{D}_m$.

(*a*) We need only show that $\mathbf{D}_m$ is complemented. Let x be in $\mathbf{D}_m$ and let $x' = m/x$. Since m is a product of distinct primes, x and x' have different prime divisors. Hence $x * x' = \gcd(x, x') = 1$ and $x + x' = \text{lcm}(x, x') = m$. Recall that 1 is the zero element (lower bound) of $\mathbf{D}_m$ and that m is the identity element (upper bound) of $\mathbf{D}_m$. Thus x' is a complement of x, and so $\mathbf{D}_m$ is a Boolean algebra.

(*b*) The atoms of $\mathbf{D}_m$ are the prime divisors of m.

15.3. Consider the Boolean algebra $\mathbf{D}_{210}$.

(*a*) List its elements and draw its diagram.

(*b*) Find the set A of atoms.

(*c*) Find two subalgebras with eight elements.

(*d*) Is $X = \{1, 2, 6, 210\}$ a sublattice of $\mathbf{D}_{210}$? A subalgebra?

(*e*) Is $Y = \{1, 2, 3, 6\}$ a sublattice of $\mathbf{D}_{210}$? A subalgebra?

(*a*) The divisors of 210 are 1, 2, 3, 5, 6, 7, 10, 14, 15, 21, 30, 35, 42, 70, 105 and 210. The diagram of $\mathbf{D}_{210}$ appears in Fig. 15-21.

(*b*) $A = \{2, 3, 5, 7\}$, the set of prime divisors of 210.

(*c*) $B = \{1, 2, 3, 35, 6, 70, 105, 210\}$ and $C = \{1, 5, 6, 7, 30, 35, 42, 210\}$ are subalgebras of $\mathbf{D}_{210}$.

(*d*) X is a sublattice since it is linearly ordered. However, X is not a subalgebra since 35 is the complement of 2 in $\mathbf{D}_{210}$ but 35 does not belong to X. (In fact, no Boolean algebra with more than two elements is linearly ordered.)

(*e*) Y is a sublattice of $\mathbf{D}_{210}$ since it is closed under $+$ and $*$. However, Y is not a subalgebra of $\mathbf{D}_{210}$ since it is not closed under complements in $\mathbf{D}_{210}$, e.g., $35 = 2'$ does not belong to Y. (We note that Y itself is a Boolean algebra; in fact, $Y = \mathbf{D}_6$.)

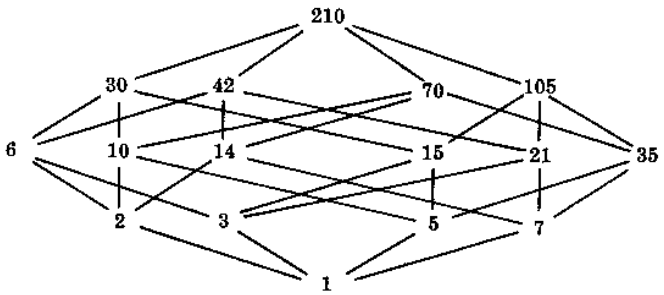


Fig. 15-21

15.4. Find the number of subalgebras of $\mathbf{D}_{210}$.

A subalgebra of $\mathbf{D}_{210}$ must contain two, four, eight or sixteen elements.

(i) There can be only one two-element subalgebra which consists of the upper bound 210 and lower bound 1, i.e., $\{1, 210\}$.

(ii) Since $\mathbf{D}_{210}$ contains sixteen elements, the only sixteen-element subalgebra is $\mathbf{D}_{210}$ itself.

(iii) Any four-element subalgebra is of the form $\{1, x, x', 210\}$, i.e., consists of the upper and lower bounds and a nonbound element and its complement. There are fourteen nonbound elements in $\mathbf{D}_{210}$ and so there are $14/2 = 7$ pairs $\{x, x'\}$. Thus $\mathbf{D}_{210}$ has seven four-element subalgebras.

(iv) Any eight-element subalgebra S will itself contain three atoms s_1, s_2, s_3. We can choose S_1 and S_2 to be any two of the four atoms of $\mathbf{D}_{210}$ and then s_3 must be the product of the other two atoms, e.g., we can let $s_1 = 2$, $s_2 = 3$, $s_3 = 5 \cdot 7 = 35$ (which determines the subalgebra B above), or we can let $s_1 = 5$, $s_2 = 7$, $s_3 = 2 \cdot 3 = 6$ (which determines the subalgebra C above). There are $\binom{4}{2} = 6$ ways to choose s_1 and s_2 from the four atoms of $\mathbf{D}_{210}$ and so $\mathbf{D}_{210}$ has six eight-element subalgebras.

Accordingly, $\mathbf{D}_{210}$ has $1 + 1 + 7 + 6 = 15$ subalgebras.

15.5. Prove Theorem 15.2: Let a, b, c be any elements in a Boolean algebra B.

(i) Idempotent laws:

(5a) $a + a = a$ (5b) $a * a = a$

(ii) Boundedness laws:

(6a) $a + 1 = 1$ (6b) $a * 0 = 0$

(iii) Absorption Laws:

(7a) $a + (a * b) = a$ (7b) $a * (a + b) = a$

(iv) Associative Laws:

(8a) $(a + b) + c = a + (b + c)$ (8b) $(a * b) * c = a * (b * c)$

(5b) $a = a * 1 = a * (a + a') = (a * a) + (a * a') = (a * a) + 0 = a * a$

(5a) Follows from (5b) and duality.

(6b) $a * 0 = (a * 0) + 0 = (a * 0) + (a * a') = a * (0 + a') = a * (a' + 0) = a * a' = 0$

(6a) Follows from (6b) and duality.

(7b) $a * (a + b) = (a + 0) * (a + b) = a + (0 * b) = a + (b * 0) = a + 0 = a$

(7a) Follows from (7b) and duality.

(8b) Let $L = (a * b) * c$ and $R = a * (b * c)$. We need to prove that $L = R$. We first prove that $a + L = a + R$. Using the absorption laws in the last two steps,

$$a + L = a + ((a * b) * c) = (a + (a * b)) * (a + c) = a * (a + c) = a$$

Also, using the absorption law in the last step,

$$a + R = a + (a * (b * c)) = (a + a) * (a + (b * c)) = a * (a + (b * c)) = a$$

Thus $a + L = a + R$. Next we show that $a' + L = a' + R$. We have,

$$\begin{aligned} a' + L = a' + ((a * b) * c) &= (a' + (a * b)) * (a' + c) \\ &= ((a' + a) * (a' + b)) * (a' + c) = (1 * (a' + b)) * (a' + c) \\ &= (a' + b) * (a' + c) = a' + (b * c) \end{aligned}$$

Also,

$$\begin{aligned} a' + R = a' + (a * (b * c)) &= (a' + a) * (a' + (b * c)) \\ &= 1 * (a' + (b * c)) = a' + (b * c) \end{aligned}$$

Thus $a' + L = a' + R$. Consequently,

$$\begin{aligned} L = 0 + L = (a * a') + L &= (a + L) * (a' + L) = (a + R) * (a' + R) \\ &= (a * a') + R = 0 + R = R \end{aligned}$$

(8a) Follows from (8b) and duality.

15.6. Prove Theorem 15.3: Let a be any element of a Boolean algebra B.

(i) (Uniqueness of Complement) If $a + x = 1$ and $a * x = 0$, then $x = a'$.

(ii) (Involution Law) $(a')' = a$

(iii) $(9a)$ $0' = 1$. $(9b)$ $1' = 0$.

(i) We have:

$$a' = a' + 0 = a' + (a * x) = (a' + a) * (a' + x) = 1 * (a' + x) = a' + x$$

Also,

$$x = x + 0 = x + (a * a') = (x + a) * (x + a') = 1 * (x + a') = x + a'$$

Hence $x = x + a' = a' + x = a'$.

(ii) By definition of complement, $a + a' = 1$ and $a * a' = 0$. By commutativity, $a' + a = 1$ and $a' * a = 0$. By uniqueness of complement, a is the complement of a', that is, $a = (a')'$.

(iii) By boundedness law $(6a)$, $0 + 1 = 1$, and by identity axiom $(3b)$, $0 * 1 = 0$. By uniqueness of complement, 1 is the complement of 0, that is, $1 = 0'$. By duality, $0 = 1'$.

15.7. Prove Theorem 15.4: (DeMorgan's laws): $(10a)$ $(a + b)' = a' * b'$. $(10b)$ $(a * b)' = a' + b'$.

$(10a)$ We need to show that $(a + b) + (a' * b') = 1$ and $(a + b) * (a' * b') = 0$; then by uniqueness of complement, $a' * b' = (a + b')$. We have:

$$\begin{aligned}(a + b) + (a' * b') &= b + a + (a' * b') = b + (a + a') * (a + b') \\ &= b + 1 * (a + b') = b + a + b' = b + b' + a = 1 + a = 1\end{aligned}$$

Also,

$$\begin{aligned}(a + b) * (a' * b') &= ((a + b) * a') * b' \\ &= ((a * a') + (b * a')) * b' = (0 + (b * a')) * b' \\ &= (b * a') * b' = (b * b') * a' = 0 * a' = 0\end{aligned}$$

Thus $a' * b' = (a + b)'$.

$(10b)$ Principle of duality (Theorem 15.1).

15.8. Prove Theorem 15.5: The following are equivalent in a Boolean algebra:

(1) $a + b = b$, (2) $a * b = a$, (3) $a' + b = 1$, (4) $a * b' = 0$.

By Theorem 14.4, (1) and (2) are equivalent. We show that (1) and (3) are equivalent. Suppose (1) holds. Then

$$a' + b = a' + (a + b) = (a' + a) + b = 1 + b = 1$$

Now suppose (3) holds. Then

$$a + b = 1 * (a + b) = (a' + b) * (a + b) = (a' * a) + b = 0 + b = b$$

Thus (1) and (3) are equivalent.

We next show that (3) and (4) are equivalent. Suppose (3) holds. By DeMorgan's law and involution,

$$0 = 1' = (a' + b')' = a'' * b' = a * b'$$

Conversely, if (4) holds then

$$1 = 0' = (a * b')' = a' + b'' = a' + b$$

Thus (3) and (4) are equivalent. Accordingly, all four are equivalent.

15.9. Prove Theorem 15.6: The mapping $f: B \to P(A)$ is an isomorphism where B is a Boolean algebra, $P(A)$ is the power set of the set A of atoms, and

$$f(x) = \{a_1, a_2, \ldots, a_n\}$$

where $x = a_1 + \cdots + a_n$ is the unique representation of a as a sum of atoms.

Recall (Chapter 14) that if the a's are atoms then $a_i^2 = a_i$ but $a_i a_j = 0$ for $a_i \neq a_j$. Suppose x, y are in B and suppose

$$x = a_1 + \cdots + a_r + b_1 + \cdots + b_s$$
$$y = b_1 + \cdots + b_s + c_1 + \cdots + c_t$$

where

$$A = \{a_1, \ldots, a_r, b_1, \ldots, b_s, c_1, \ldots, c_t, d_1, \ldots, d_k\}$$

is the set of atoms of B. Then

$$x + y = a_1 + \cdots + a_r + b_1 + \cdots + b_s + c_1 + \cdots + c_t$$
$$xy = b_1 + \cdots + b_s$$

Hence

$$\begin{aligned} f(x+y) &= \{a_1, \ldots, a_r, b_1, \ldots, b_s, c_1, \ldots, c_t\} \\ &= \{a_1, \ldots, a_r, b_1, \ldots, b_s\} \cup \{b_1, \ldots, b_s, c_1, \ldots, c_t\} \\ &= f(x) \cup f(y) \\ f(xy) &= \{b_1, \ldots, b_s\} \\ &= \{a_1, \ldots, a_r, b_1, \ldots, b_s\} \cap \{b_1, \ldots, b_s, c_1, \ldots, c_t\} \\ &= f(x) \cap f(y) \end{aligned}$$

Let

$y = c_1 + \cdots + c_t + d_1 + \cdots + d_k$. Then $x + y = 1$ and $xy = 0$, and so $y = x'$

Thus

$$f(x') = \{c_1, \ldots, c_t, d_1, \ldots, d_k\} = \{a_1, \ldots, a_r, b_1, \ldots, b_s\}^c = (f(x))^c$$

Since the representation is unique, f is one-to-one and onto. Hence f is a Boolean algebra isomorphism.

BOOLEAN EXPRESSIONS

15.10. Reduce the following Boolean products to either 0 or a fundamental product:

(*a*) $xyx'z$; (*b*) $xyzy$; (*c*) $xyz'yx$; (*d*) $xyz'yx'z'$.

Use the commutative law $x * y = y * x$, the complement law $x * x' = 0$, and the idempotent law $x * x = x$:

(*a*) $zyx'z = xx'yz = 0yz = 0$

(*b*) $xyzy = xyyz = xyz$.

(*c*) $xyz'yx = xxyyz' = xyz'$.

(*d*) $xyz'yx'z' = xx'yyz'z' = 0yz' = 0$.

15.11. Express each Boolean expression $E(x, y, z)$ as a sum-of-products and then in its complete sum-of-products form: (*a*) $E = x(xy' + x'y + y'z)$; (*b*) $E = z(x' + y) + y'$.

First use Algorithm 15.8A to express E as a sum-of-products, and then use Algorithm 15.8B to express E as a complete sum-of-products.

(*a*) First we have $E = xxy' + xx'y + xy'z = xy' + xy'z$. Then

$$E = xy'(z + z') + xy'z = xy'z + xy'z' + xy'z = xy'z + xy'z'$$

(*b*) First we have

$$E = z(x' + y) + y' = x'z + yz + y'$$

Then

$$\begin{aligned} E = x'z + yz + y' &= x'z(y + y') + yz(x + x') + y'(x + x')(z + z') \\ &= x'yz + x'y'z + xyz + x'yz + xy'z + xy'z' + x'y'z + x'y'z \\ &= xyz + xy'z + xy'z' + x'yz + x'y'z + x'y'z' \end{aligned}$$

15.12. Express $E(x, y, z) = (x' + y)' + x'y$ in its complete sum-of-products form.

We have $E = (x' + y)' + x'y = xy' + x'y$, which would be the complete sum-of-products form of E if E were a Boolean expression in x and y. However, it is specified that E is a Boolean expression in the three variables x, y, and z. Hence,

$$E = xy' + x'y = xy'(z + z') + x'y(z + z') = xy'z + xy'z' + x'yz + x'yz'$$

is the complete sum-of-products form of E.

15.13. Express each Boolean expression $E(x, y, z)$ as a sum-of-products and then in its complete sum-of-products form: (*a*) $E = y(x + yz)'$; (*b*) $E = x(xy + y' + x'y)$.

(*a*) $E = y(x'(yz)') = yx'(y' + z') = yx'y' + x'yz' = x'yz'$

which already is in its complete sum-of-products form.

(*b*) First we have $E = xxy + xy' + xx'y = xy + xy'$. Then

$$E = xy(z + z') + xy'(z + z') = xyz + xyz' + xy'z + xy'z'$$

15.14. Express each set expression $E(A, B, C)$ involving sets A, B, C as a union of intersections:

(*a*) $E = (A \cup B)^c \cap (C^c \cup B)$; (*b*) $E = (B \cap C)^c \cap (A^c \cap C)^c$

Use Boolean notation, $'$ for complement, $+$ for union and $*$ (or juxtaposition) for intersection, and then express E as a sum of products (union of intersections).

(*a*) $E = (A + B)'(C' + B) = A'B'(C' + B) = A'B'C' + A'B'B = A'B'C'$ or $E = A^c \cap B^c \cap C^c$.

(*b*) $E = (BC)'(A' + C)' = (B' + C')(AC') = AB'C' + AC'$ or $E = (A \cap B^c \cap C^c) \cup (A \cap C^c)$.

15.15. Let $E = xy' + xyz' + x'yz'$. Prove that (*a*) $xz' + E = E$; (*b*) $x + E \neq E$; (*c*) $z' + E \neq E$.

Since the complete sum-of-products form is unique, $A + E = E$, where $A \neq 0$, if and only if the summands in the complete sum-of-products form for A are among the summands in the complete sum-of-products form for E. Hence, first find the complete sum-of-products form for E:

$$E = xy'(z + z') + xyz' + x'yz' = xy'z + xy'z' + xyz' + x'yz'$$

(a) Express xz' in complete sum-of-products form:

$$xz' = xz'(y + y') = xyz' + xy'z'$$

Since the summands of xz' are among those of E, we have $xz' + E = E$.

(b) Express x in complete sum-of-products form:

$$x = x(y + y')(z + z') = xyz + xyz' + xy'z + xy'z'$$

The summand xyz of x is not a summand of E; hence $x + E \neq E$.

(c) Express z' in complete sum-of-products form:

$$z' = z'(x + x')(y + y') = xyz' + xy'z' + x'yz' + x'y'z'$$

The summand $x'y'z'$ of z' is not a summand of E; hence $z' + E \neq E$.

MINIMAL BOOLEAN EXPRESSIONS, PRIME IMPLICANTS

15.16. For any Boolean sum-of-products expression E, we let E_L denote the number of literals in E (counting multiplicity) and E_S denote the number of summands in E. Find E_L and E_S for each of the following:

(a) $E = xy'z + x'z' + yz' + x$. (c) $E = xyt' + x'y'zt + xz't$.

(b) $E = x'y'z + xyz + y + yz' + x'z$. (d) $E = (xy' + z)' + xy'$.

Simply add up the number of literals and the number of summands in each expression:

(a) $E_L = 3 + 2 + 2 + 1 - 8$, $E_S = 4$.

(b) $E_L = 3 + 3 + 1 + 2 + 2 = 11$, $E_S = 5$.

(c) $E_L = 3 + 4 + 3 = 10$, $E_S = 3$.

(d) Because E is not written as a sum of products, E_L and E_S are not defined.

15.17. Given that E and F are equivalent Boolean sum-of-products, define:
(a) E is simpler than F; (b) E is minimal.

(a) E is simpler than F if $E_L < F_L$ and $E_S \leq F_S$, or if $E_L \leq F_L$ and $E_S < F_S$.

(b) E is minimal if there is no equivalent sum-of-products expression which is simpler than E.

15.18. Find the consensus Q of the fundamental products P_1 and P_2 where:

(a) $P_1 = xy'z'$, $P_2 = xyt$. (c) $P_1 = xy'z'$, $P_2 = x'y'zt$.

(b) $P_1 = xyz't$, $P_2 = xzt$. (d) $P_1 = xyz'$, $P_2 = xz't$.

The consensus Q of P_1 and P_2 exists if there is exactly one variable, say x_k, which is complemented in one of P_1 and P_2 and uncomplemented in the other. Then Q is the product (without repetition) of the literals in P_1 and P_2 after x_k and x_k' have been deleted.

(a) Delete y' and y and then multiply the literals of P_1 and P_2 (without repetition) to obtain $Q = xz't$.

(b) Deleting z' and z yields $Q = xyt$.

(c) They have no consensus since both x and z appear complemented in one of the products and uncomplemented in the other.

(d) They have no consensus since no variable appears complemented in one of the products and uncomplemented in the other.

15.19. Prove Lemma 15.10: Suppose Q is the consensus of P_1 and P_2. Then $P_1 + P_2 + Q = P_1 + P_2$.

Since the literals commute, we can assume without loss of generality that

$$P_1 = a_1a_2 \cdots a_r, t, \qquad P_2 = b_1b_2 \cdots b_st', \qquad Q = a_1a_2 \cdots a_rb_1b_2 \cdots b_s$$

Now, $Q = Q(t + t') = Qt + Qt'$. Because Qt contains P_1, $P_1 + Qt = P_1$; and because Qt' contains P_2, $P_2 + Qt' = P_2$. Hence

$$P_1 + P_2 + Q = P_1 + P_2 + Qt + Qt' = (P_1 + Qt) + (P_2 + Qt') = P_1 + P_2$$

15.20. Let $E = xy' + xyz' + x'yz'$. Find: (*a*) the prime implicants of E; (*b*) a minimal sum for E.

(*a*) Apply Algorithm 15.9A (consensus method) as follows:

$$\begin{aligned} E &= xy' + xyz' + x'yz' + xz' && \text{(consensus of } xy' \text{ and } xyz') \\ &= xy' + x'yz' + xz' && (xyz' \text{ includes } xz') \\ &= xy' + x'yz' + xz' + yz' && \text{(consensus of } x'yz' \text{ and } xz') \\ &= xy' + xz' + yz' && (x'yz' \text{ includes } yz') \end{aligned}$$

Neither step in the consensus method can now be applied. Hence xy', xz', and yz' are the prime implicants of E.

(*b*) Apply Algorithm 15.9B. Write each prime implicant of E in complete sum-of-products form obtaining:

$$\begin{aligned} xy' &= xy'(z + z') = xy'z + xy'z' \\ xz' &= xz'(y + y') = xyz' + xy'z' \\ yz' &= yz'(x + x') = xyz' + x'yz' \end{aligned}$$

Only the summands xyz' and $xy'z'$ of xz' appear among the other summands and hence xz' can be eliminated as superfluous. Thus $E = xy' + yz'$ is a minimal sum for E.

15.21. Let $E = xy + y't + x'yz' + xy'zt'$. Find: (*a*) prime implicants of E; (*b*) minimal sum for E.

(*a*) Apply Algorithm 15.9A (consensus method) as follows:

$$\begin{aligned} E &= xy + y't + x'yz' + xy'zt' + xzt' && \text{(consensus of } xy \text{ and } xy'zt') \\ &= xy + y't + x'yz' + xzt' && (xy'zt' \text{ includes } xzt') \\ &= xy + y't + x'yz' + xzt' + yz' && \text{(consensus of } xy \text{ and } x'yz') \\ &= xy + y't + xzt' + yz' && (x'yz' \text{ includes } yz') \\ &= xy + y't + xzt' + yz' + xt && \text{(consensus of } xy \text{ and } y't) \\ &= xy + y't + xzt' + yz' + xt + xz && \text{(consensus of } xzt' \text{ and } xt) \\ &= xy + y't + yz' + xt + xz && (xzt' \text{ includes } xz) \\ &= xy + y't + yz' + xt + xz + z' && \text{(consensus of } y't \text{ and } yz') \end{aligned}$$

Neither step in the consensus method can now be applied. Hence the prime implicants of E are xy, $y't$, yz', xt, xz, and $z't$.

(*b*) Apply Algorithm 15.9B, that is, write each prime implicant in complete sum-of-products form and then delete one by one those which are superfluous, i.e. those whose summands appear among the other summands. This finally yields

$$E = y't + xz + yz'$$

as a minimal sum for E.

LOGIC GATES

15.22. Express the output Y as a Boolean expression in the inputs A, B, C for the logic circuit in: (a) Fig. 15-22(a); (b) Fig. 15-22(b).

(a) The inputs to the first AND gate are A and B' and to the second AND gate are B' and C. Thus $Y = AB' + B'C$.

(b) The inputs to the first AND gate are A and B' and to the second AND gate are A' and C. Thus $Y = AB' + A'C$.

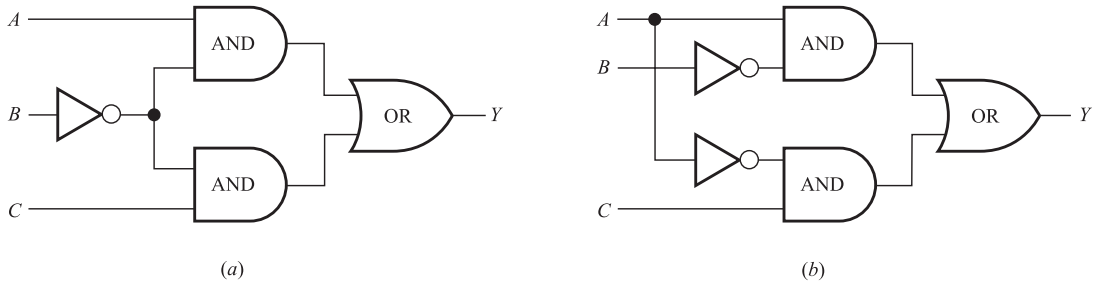


Fig. 15-22

15.23. Express the output Y as a Boolean expression in the inputs A, B, C for the logic circuit in Fig. 15-23.

The output of the first AND gate is $A'BC$, of the second AND gate is $AB'C'$, and of the last AND gate is AB'. Thus

$$Y = A'BC + AB'C' + AB'$$

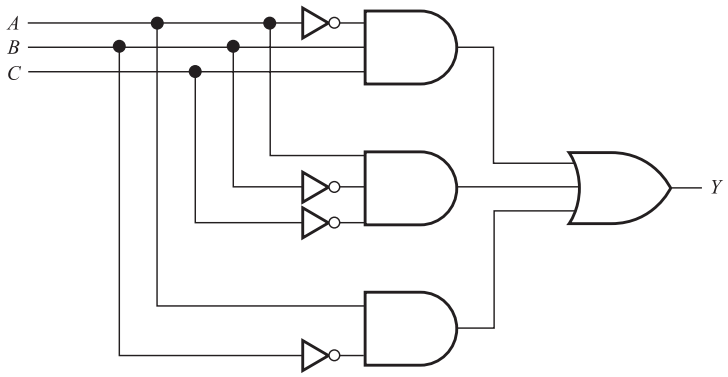


Fig. 15-23

15.24. Express the output Y as a Boolean expression in the inputs A, B, C for the logic circuit in: (a) Fig. 15-24(a); (b) Fig. 15-24(b).

(a) The output of the AND gate is BC and so the inputs to the NOR gate are A and BC. Thus $(A + BC)'$ is the output of the NOR gate. Therefore, the inputs to the OR gate are $(A + BC)'$ and B; hence $Y = (A + BC)' + B$.

(*b*) The output of the NAND gate is $(A'B)'$ and the output of the NOR gate is $(A + C)'$. Thus $Y = (A'B)' + (A + C)'$.

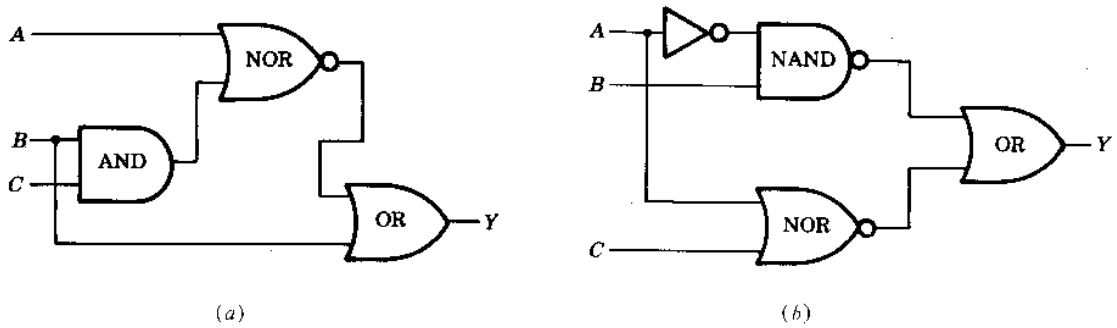


Fig. 15-24

15.25. Express the output Y as a Boolean expression in the inputs A and B for the logic circuit in Fig. 15-25.

Here a small circle in the circuit means complement. Thus the output of the three gates on the left are AB', $(A + B)'$, and $(A'B)'$ Hence

$$Y = AB' + (A + B)' + (A'B)'$$

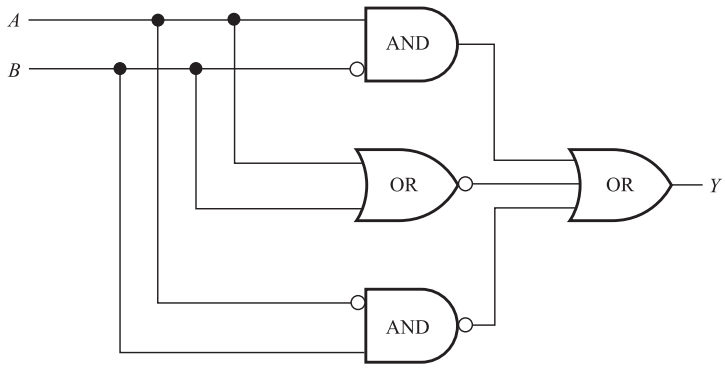
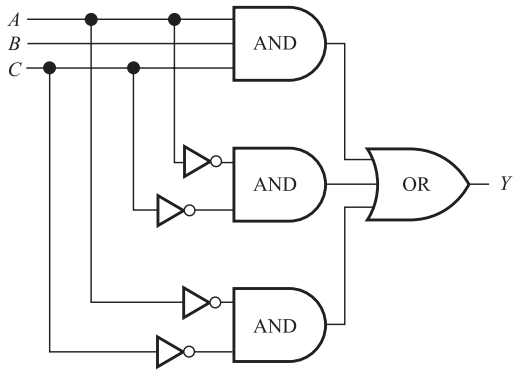


Fig. 15-25

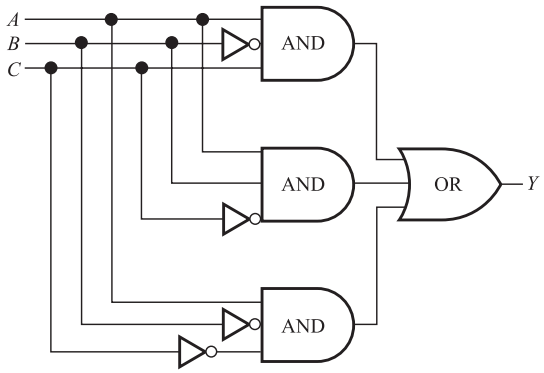
15.26. Draw the logic circuit L with inputs A, B, C and output Y which corresponds to each Boolean expression:

(*a*) $Y = ABC + A'C' + B'C'$; (*b*) $Y = AB'C + ABC' + AB'C'$.

These are sum-of-products expressions. Thus L will be an AND-OR circuit which has an AND gate for each product and one OR gate for the sum. The required circuits appear in Fig. 15-26(*a*) and (*b*).



(*a*) $Y = ABC + A'C' + B'C'$



(*b*) $Y = AB'C + ABC' + AB'C'$

Fig. 15-26

TRUTH TABLES

15.27. Find the ouptut sequence Y for an AND gate with inputs A, B, C (or equivalently for $Y = ABC$) where:

(*a*) $A = 111001$; $B = 100101$; $C = 110011$.

(*b*) $A = 11111100$; $B = 10101010$; $C = 00111100$.

(*c*) $A = 00111111$; $B = 11111100$; $C = 11000011$.

The output $Y = 1$ for an AND gate if and only if there are 1's in all the positions of the input sequences. Thus:

(*a*) Only the first and last positions have 1's in all three sequences. Hence $Y = 100001$.

(*b*) Only the third and fifth positions (reading from left to right) have 1's in all three sequences. Thus $Y = 00101000$.

(*c*) No position has 1's in all three sequences. Thus $Y = 00000000$.

15.28. Find the output sequence Y for an OR gate with inputs A, B, C (or equivalently for $Y = A + B + C$) where:

(*a*) $A = 100001$; $B = 100100$; $C = 110000$.

(*b*) $A = 11000000$; $B = 10101010$; $C = 00000011$.

(*c*) $A = 00111111$; $B = 11111100$; $C = 11000011$.

The output $Y = 0$ for an OR gate if and only if there are 0's in all the positions of the input sequences. Thus:

(*a*) Only the third and fifth positions have 0's in all three sequences. Hence $Y = 110101$.

(*b*) Only the fourth and sixth positions (reading from left to right) have 0's in all three sequences. Thus $Y = 11101011$.

(*c*) No position has 0's in all three sequences. Thus $Y = 11111111$.

15.29. Find the output sequence Y for a NOT gate with input A or, equivalently, for $Y = A'$, where:

(*a*) $A = 00111111$; (*b*) $A = 11111100$; (*c*) $A = 11000011$.

The NOT gate changes 0 to 1 and 1 to 0. Hence:

(*a*) $A' = 11000000$; (*b*) $A' = 00000011$; (*c*) $A' = 00111100$.

15.30. Consider a logic circuit L with $n = 5$ inputs A, B, C, D, E or, equivalently, consider a Boolean expression E with five variables x_1, x_2, x_3, x_4, x_5.

(*a*) Find the special sequences for the variables (inputs).

(*b*) How many different ways can we assign a bit (0 or 1) to each of the $n = 5$ variables?

(*c*) What is the main property of the special sequences?

(*a*) All sequences have length $2^n = 2^5 = 32$. They will consist of alternating blocks of 0s and 1s where the lengths of the blocks are $2^{n-1} = 2^4 = 16$ for x_1, $2^{n-2} = 2^3 = 8$ for $x_2, \ldots, 2^{n-5} = 2^0 = 1$ for x_5, Thus:

$$x_1 = 00000000000000001111111111111111$$
$$x_2 = 00000000111111110000000011111111$$
$$x_3 = 00001111000011110000111100001111$$
$$x_4 = 00110011001100110011001100110011$$
$$x_5 = 01010101010101010101010101010101$$

(*b*) There are two ways, 0 or 1, to assign a bit to each variable, and so there are $2^n = 2^5 = 32$ ways of assigning a bit to each of the $n = 5$ variables.

(*c*) The 32 positions in the special sequences give all the 32 possible combinations of bits for the five variables.

15.31. Find the truth table $T = T(E)$ for the Boolean expression $E = E(x, y, z)$ where:

(*a*) $E = xz + x'y$; (*b*) $E = xy'z + xy + z'$.

The special sequences for the variables x, y, z and their complements follow:

$$x = 00001111, \quad y = 00110011, \quad z = 01010101$$
$$x' = 11110000, \quad y' = 11001100, \quad z' = 10101010$$

(*a*) Here $xz = 00000101$ and $x'y = 00110000$. Then $E = xz + x'y = 00110101$. Thus

$$T(00001111,\ 00110011,\ 01010101) = 00110101$$

or simply $T(E) = 00110101$ where we assume the input consists of the special sequences.

(*b*) Here $xy'z = 00000100$, $xy = 00000011$, and $z' = 01010101$. Then $E = xy'z + xy + z' = 01010111$. Thus

$$T(00001111,\ 00110011,\ 01010101) = 01010111$$

15.32. Find the truth table $T = T(E)$ for the Boolean expression $E = E(x,\ y,\ z)$ where:

(*a*) $E = xyz' + x'yz$; (*b*) $E = xyz + xy'z + x'y'z$.

Here E is a complete sum-of-products expression which is the sum of minterms. Example 15.13 gives the truth tables for the minterms (using the special sequences). Each minterm contains a single 1 in its truth table; hence the truth table of E will have 1s in the same positions as the 1s in the minterms in E. Thus:

(*a*) $T(E) = 00001010$; (*b*) $T(E) = 01000101$

15.33. Find the truth table $T = T(E)$ for the Boolean expression

$$E = E(x,\ y,\ z) = (x'y)'yz' + x'(yz + z')$$

First express E as a sum-of-products:

$$E = (x + y')yz' + x'yz + x'z' = xyz' + y'yz' + x'yz + x'z' = xyz' + x'yz + x'z'$$

Now express E as a complete sum-of-products:

$$E = xyz' + x'yz + x'z'(y + y') = xyz' + x'yz + x'yz' + x'y'z'$$

As in Problem 15.32, use the truth tables for the minterms appearing in Example 15.13 to obtain $T(E) = 10101010$.

15.34. Find the Boolean expression $E = E(x, y, z)$ corresponding to the truth table:
(*a*) $T(E) = 01001001$; (*b*) $T(E) = 00010001$.

Each 1 in $T(E)$ corresponds to the minterm with the 1 in the same position (using the truth tables for the minterms appearing in Example 15.13). For example, the 1 in the second position corresponds to $x'y'z$ whose truth table has a single 1 in the second position. Then E is the sum of these minterms. Thus:

(*a*) $E = x'y'z + x'yz + xyz'$; (*b*) $E = xy'z' + xyz$

(Again we assume the input consists of the special sequences.)

KARNAUGH MAPS

15.35. Find the fundamental product P represented by each basic rectangle in the Karnaugh map in Fig. 15-27.

In each case find those literals which appear in all the squares of the basic rectangle; then P is the product of such literals.

(*a*) x' and z' appear in both squares; hence $P = x'z'$.

(*b*) x and z appear in both squares; hence $P = xz$.

(*c*) Only z appears in all four squares; hence $P = z$.

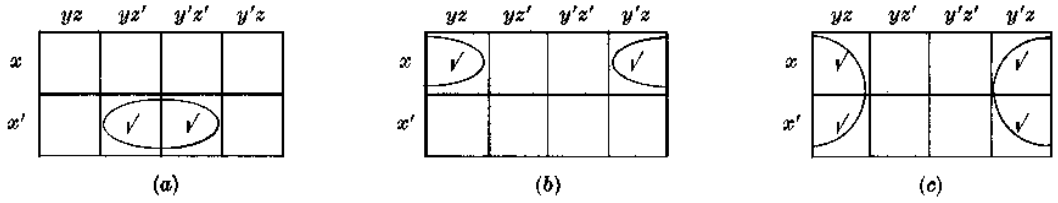


Fig. 15-27

15.36. Let R be a basic rectangle in a Karnaugh map for four variables x, y, z, t. State the number of literals in the fundamental product P corresponding to R in terms of the number of squares in R.

P will have one, two, three, or four literals according as R has eight, four, two, or one squares.

15.37. Find the fundamental product P represented by each basic rectangle R in the Karnaugh map in Fig. 15-28.

In each case find those literals which appear in all the squares of the basic rectangle; then P is the product of such literals. (Problem 15.36 indicates the number of such literals in P.)

(*a*) There are two squares in R, so P has three literals. Specifically, x', y', t' appear in both squares; hence $P = x'y't'$.

(*b*) There are four squares in R, so P has two literals. Specifically, only y' and t appear in all four squares; hence $P = y't$.

(*c*) There are eight squares in R, so P has only one literal. Specifically, only y appears in all eight squares; hence $P = y$.

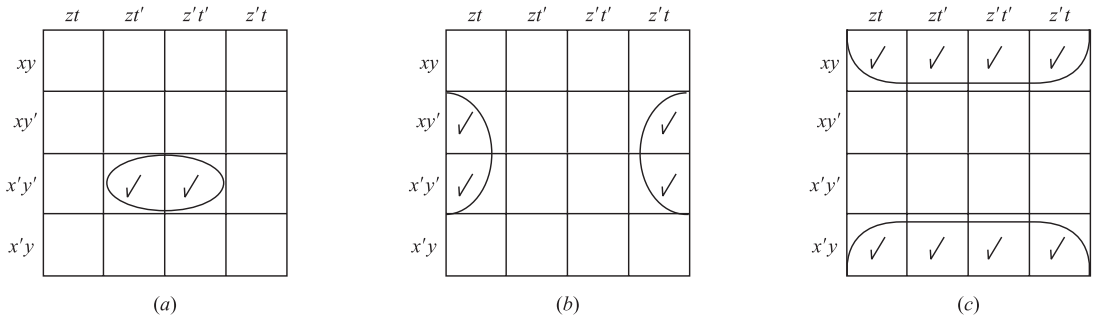


Fig. 15-28

15.38. Let E be the Boolean expression given in the Karnaugh map in Fig. 15-29.
(*a*) Write E in its complete sum-of-products form. (*b*) Find a minimal form for E.

(*a*) List the seven fundamental products checked to obtain

$$E = xyz't' + xyz't + xy'zt + xy'zt' + x'y'zt + x'y'zt' + x'yz't'$$

(*b*) The two-by-two maximal basic rectangle represents $y'z$ since only y' and z appear in all four squares. The horizontal pair of adjacent squares represents xyz', and the adjacent squares overlapping the top and bottom edges represent $yz't'$. As all three rectangles are needed for a minimal cover,

$$E = y'z + xyz' + yz't'$$

is the minimal sum for E.

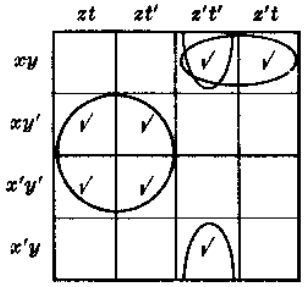


Fig. 15-29

15.39. Consider the Boolean expressions E_1 and E_2 in variables x, y, z, t which are given by the Karnaugh maps in Fig. 15-30. Find a minimal sum for (*a*) E_1; (*b*) E_2.

(*a*) Only y' appears in all eight squares of the two-by-four maximal basic rectangle, and the designated pair of adjacent squares represents xzt'. As both rectangles are needed for a minimal cover,

$$E_1 = y' + xzt'$$

is the minimal sum for E_1.

(*b*) The four corner squares form a two-by-two maximal basic rectangle which represents yt, since only y and t appear in all the four squares. The four-by-one maximal basic rectangle represents $x'y'$, and the two adjacent squares represent $y'zt'$. As all three rectangles are needed for a minimal cover,

$$E_2 = yt + x'y' + y'zt'$$

is the minimal sum for E_2.

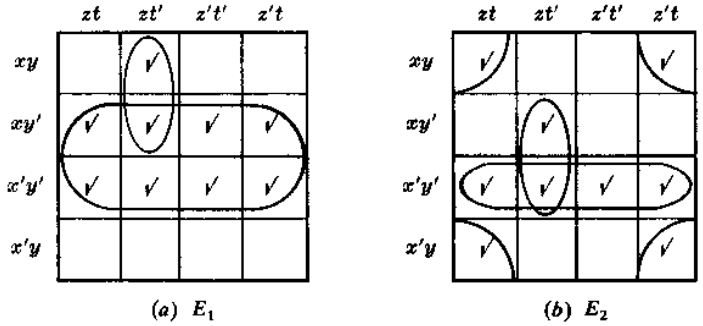


Fig. 15-30

15.40. Consider the Boolean expressions E_1 and E_2 in variables x, y, z, t which are given by the Karnaugh maps in Fig. 15-31. Find a minimal sum for (*a*) E_1; (*b*) E_2.

(*a*) There are five prime implicants, designated by the four loops and the dashed circle. However, the dashed circle is not needed to cover all the squares, whereas the four loops are required. Thus the four loops give the minimal sum for E_1; that is,

$$E_1 = xzt' + xy'z' + x'y'z + x'z't'$$

(*b*) There are five prime implicants, designated by the five loops of which two are dashed. Only one of the two dashed loops is needed to cover the square $x'y'z't'$. Thus there are two minimal sums for E_2 as follows:

$$E_2 = x'y + yt + xy't' + y'z't' = x'y + yt + xy't' + x'z't'$$

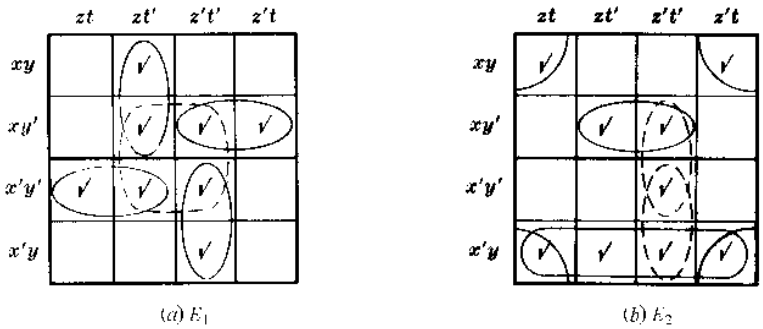


Fig. 15-31

15.41. Use a Karnaugh map to find a minimal sum for:

(*a*) $E_1 = x'yz + x'yz't + y'zt' + xyzt' + xy'z't'$.

(*b*) $E_2 = y't' + y'z't + x'y'zt + yzt'$.

(*a*) Check the two squares corresponding to each of $x'yz$ and $y'zt'$, and check the square corresponding to each of $x'yz't$, $xyzt'$, and $xy'z't'$. This gives the Karnaugh map in Fig. 15-32(*a*). A minimal cover consists of the three designated loops. Thus a minimal sum for E_1 follows:

$$E_1 = zt' + xy't' + x'yt$$

(*b*) Check the four squares corresponding to zt', check the two squares corresponding to each of $y'z't$ and yzt', and check the square corresponding to $x'y'zt$. This gives the Karnaugh map in Fig. 15-32(*b*). A minimal cover consists of the three designated maximal basic rectangles. Thus a minimal sum for E_2 follows:

$$E_2 = zt' + xy't' + x'yt$$

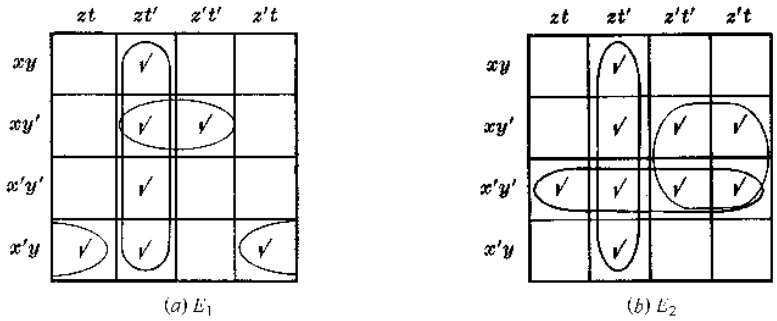


Fig. 15-32

15.42. Find a minimal sum-of-products form for the Boolean expression E with the following truth tables:

(*a*) $T(00001111, 00110011, 01010101) = 10100110$.

(*b*) $T(00001111, 00110011, 01010101) = 00101111$.

(*a*) From the given truth table T (and the truth tables in Example 15.13 for the minterms in variables x, y, z) we can read off the complete sum-of-products form for E:

$$E = x'y'z' + x'yz' + xy'z + xyz'$$

Its Karnaugh map appears in Fig. 15-33(*a*). There are three prime implicants, as indicated by the three loops, which form a minimal cover of E. Thus a minimal form for E follows:

$$E = yz' + x'z' + xy'z$$

(*b*) From the given truth table we can read off the complete sum-of-products form for E:

$$E = x'yz' + x'yz + xy'z + xyz' + xyz$$

Its Karnaugh map appears in Fig. 15-33(*b*). There are two prime implicants, as indicated by the two loops, which form a minimal cover of E. Thus a minimal form for E follows:

$$E = xz + y$$

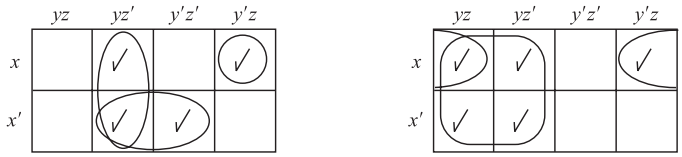


Fig. 15-33

Supplementary Problems

BOOLEAN ALGEBRAS

15.43. Write the dual of each Boolean expression:

(*a*) $a(a' + b) = ab$.

(*b*) $(a + 1)(a + 0) = a$.

(*c*) $(a + b)(b + c) = ac + b$.

15.44. Consider the lattices $\mathbf{D}_m$ of divisors of m (where $m > 1$).

(*a*) Show that $\mathbf{D}_m$ is a Boolean algebra if and only if m is *square-free*, that is, if m is a product of distinct primes.

(*b*) If $\mathbf{D}_m$ is a Boolean algebra, show that the atoms are the distinct prime divisors of m.

15.45. Consider the following lattices: (*a*) $\mathbf{D}_{20}$; (*b*) $\mathbf{D}_{55}$; (*c*) $\mathbf{D}_{99}$; (*d*) $\mathbf{D}_{130}$. Which of them are Boolean algebras, and what are their atoms?

15.46. Consider the Boolean algebra $\mathbf{D}_{110}$. (*a*) List its elements and draw its diagram. (*b*) Find all its sublattices. (*c*) Find the number of sublattices with four elements. (*d*) Find the set A of atoms of $\mathbf{D}_{110}$. (*e*) Give the isomorphic mapping $f: \mathbf{D}_{110} \to P(A)$ as defined in Theorem 15.6.

15.47. Let B be a Boolean algebra. Show that:

(*a*) For any x in B, $0 \leq x \leq 1$.

(*b*) $a < b$ if and only if $b' < a'$.

15.48. An element x in a Boolean algebra is called a *maxterm* if the identity 1 is its only successor. Find the maxterms in the Boolean algebra $\mathbf{D}_{210}$ pictured in Fig. 15-21.

15.49. Let B be a Boolean algebra. (*a*) Show that complements of the atoms of B are the maxterms. (*b*) Show that any element x in B can be expressed uniquely as a product of maxterms.

15.50. Let B be a 16-element Boolean algebra and let S be an 8-element subalgebra of B. Show that two of the atoms of S must be atoms of B.

15.51. Let $B = (B, +, *, ', 0, 1)$ be a Boolean algebra. Define an operation $\triangle$ on B (called the symmetric difference) by

$$x \triangle y = (x * y') + (x' * y)$$

Prove that $R = (B, \triangle, *)$ is a commutative Boolean ring. (See Section 12.6 and Problem 12.77.)

15.52. Let $R = (R, \oplus, \cdot)$ be a Boolean ring with identity $1 \neq 0$. Define

$$x' = 1 \oplus x, \qquad x + y = x \oplus y \oplus x \cdot y, \qquad x * y = x \cdot y$$

Prove that $B = (R, +, *, ', 0, 1)$ is a Boolean algebra.

BOOLEAN EXPRESSIONS, PRIME IMPLICANTS

15.53. Reduce the following Boolean products to either 0 or a fundamental product:

(*a*) $xy'zxy'$; (*b*) $xyz'sy'ts$; (*c*) $xy'xz'ty'$; (*d*) $xyz'ty't$.

15.54. Express each Boolean expression $E(x, y, z)$ as a sum-of-products and then in its complete sum-of-products form:

(*a*) $E = x(xy' + x'y + y'z)$. (*b*) $E = (x + y'z)(y + z')$. (*c*) $E = (x' + y)' + y'z$.

15.55. Express each Boolean expression $E(x, y, z)$ as a sum-of-products and then in its complete sum-of-products form:

(*a*) $E = (x'y)'(x' + xyz')$. (*b*) $E = (x + y)'(xy')'$. (*c*) $E = y(x + yz)'$.

15.56. Find the consensus Q of the fundamental products P_1 and P_2 where:

(*a*) $P_1 = xy'z$, $P_2 = xyt$. (*c*) $P_1 = xy'zt$, $P_2 = xyz'$.
(*b*) $P_1 = xyz't'$, $P_2 = xzt'$. (*d*) $P_1 = xy't$, $P_2 = xzt$.

15.57. For any Boolean sum-of-products expression E, we let E_L denote the number of literals in E (counting multiplicity) and E_S denote the number of summands in E. Find E_L and E_S for each of the following:

(*a*) $E = xyz't + x'yt + xy'zt$. (*b*) $E = xyzt + xt' + x'y't + yt$.

15.58. Apply the consensus method (Algorithm 15.9A) to find the prime implicants of each Boolean expression:

(*a*) $E_1 = xy'z' + x'y + x'y'z' + x'yz$.
(*b*) $E_2 = xy' + x'z't + xyzt' + x'y'zt'$.
(*c*) $E_3 = xyzt + xyz't' + xz't' + x'y'z' + x'yz't$.

15.59. Find a minimal sum-of-products form for each of the Boolean expressions in Problem 15.58.

LOGIC GATES, TRUTH TABLES

15.60. Express the output Y as a Boolean expression in the inputs A, B, C for the logic circuit in:
(*a*) Fig. 15-34(*a*); (*b*) Fig. 15-34(*b*).

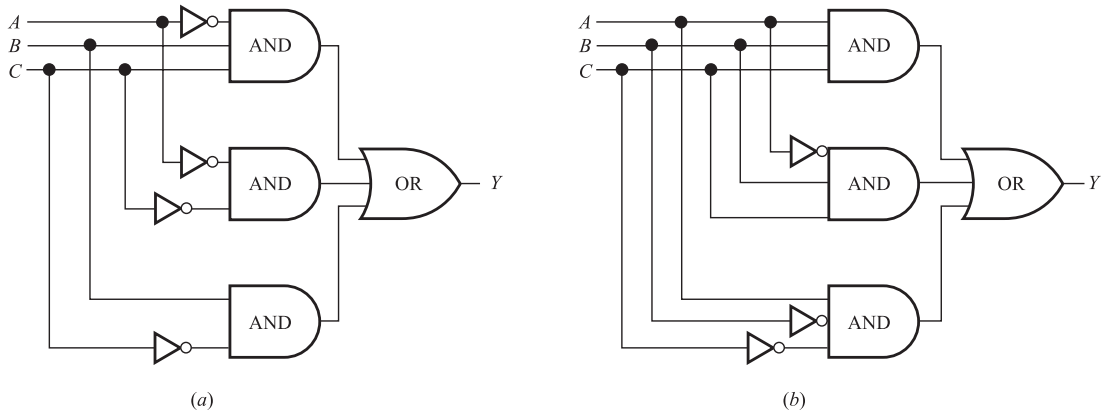


Fig. 15-34

15.61. Express the output Y as a Boolean expression in the inputs A, B, C for the logic circuit in: (*a*) Fig. 15-35(*a*); (*b*) Fig. 15-35(*b*).

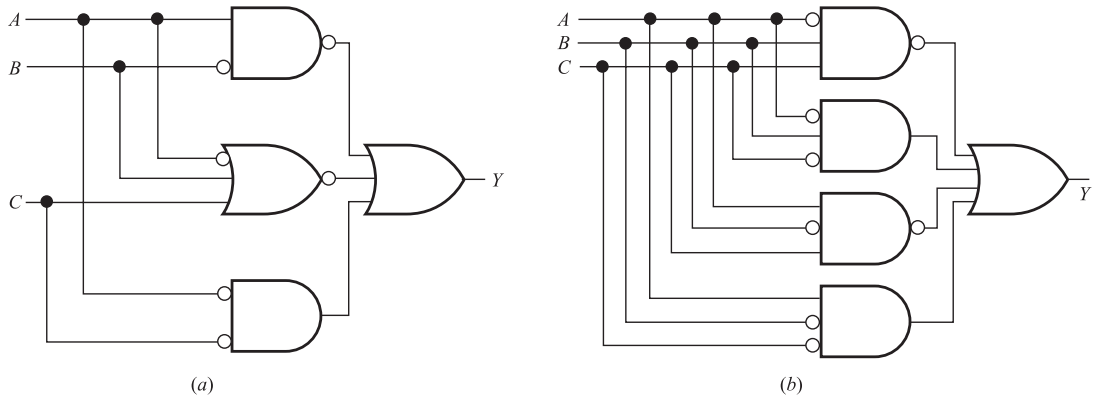


Fig. 15-35

15.62. Draw the logic circuit L with inputs A, B, C and output Y which corresponds to each Boolean expression:

(*a*) $Y = AB'C + AC' + B'C$. (*b*) $Y = A'BC + A'BC' + ABC'$

15.63. Find the output sequence Y for an AND gate with inputs A, B, C (or equivalently for $Y = ABC$) where:

(*a*) $A = 110001$; $B = 101101$; $C = 110011$.

(*b*) $A = 01111100$; $B = 10111010$; $C = 00111100$.

(*c*) $A = 00111110$; $B = 01111100$; $C = 11110011$.

15.64. Find the output sequence Y for an OR gate with inputs A, B, C (or equivalently for $Y = A + B + C$) where:

(*a*) $A = 100011$; $B = 100101$; $C = 1000001$.

(*b*) $A = 10000001$; $B = 00100100$; $C = 00000011$.

(*c*) $A = 00111100$; $B = 11110000$; $C = 10000001$.

15.65. Find the output sequence Y for a NOT gate with input A or, equivalently, for $Y = A'$, where:

(*a*) $A = 11100111$; (*b*) $A = 10001000$; (*c*) $A = 11111000$.

15.66. Consider a logic circuit L with $n = 6$ inputs A, B, C, D, E, F, or, equivalently, consider a Boolean expression E with six variables $x_1, x_2, x_3, x_4, x_5, x_6$.

(*a*) How many different ways can we assign a bit (0 or 1) to each of the $n = 6$ variables?

(*b*) Find the first three special sequences for the variables (inputs).

15.67. Find the truth table $T = T(E)$ for the Boolean expression $E = E(x, y, z)$ where:

(*a*) $E = xy + x'z$. (*b*) $E = xyz' + y + xy'$.

15.68. Find the truth table $T = T(E)$ for the Boolean expression $E = E(x, y, z)$ where:

(*a*) $E = x'yz' + x'y'z$. (*b*) $E = xyz' + xy'z' + x'y'z'$.

15.69. Find the Boolean expression $E = E(x, y, z)$ corresponding to the truth tables:

(*a*) $T(E) = 10001010$; (*b*) $T(E) = 00010001$; (*c*) $T(E) = 00110000$.

15.70. Find all possible minimal sums for each Boolean expression E given by the Karnaugh maps in Fig. 15-36.

	yz	yz'	$y'z'$	$y'z$
x	√		√	√
x'	√	√		

(*a*)

	yz	yz'	$y'z'$	$y'z$
x	√		√	√
x'	√	√		√

(*b*)

	yz	yz'	$y'z'$	$y'z$
x	√			√
x'	√	√	√	√

(*c*)

Fig. 15-36

15.71. Find all possible minimal sums for each Boolean expression E given by the Karnaugh maps in Fig. 15-37.

	zt	zt'	$z't'$	$z't$
xy		√		√
xy'	√	√		√
$x'y'$		√		
$x'y$	√	√	√	√

(*a*)

	zt	zt'	$z't'$	$z't$
xy	√	√	√	
xy'		√	√	√
$x'y'$		√		
$x'y$	√	√	√	

(*b*)

	zt	zt'	$z't'$	$z't$
xy	√			√
xy'		√	√	
$x'y'$		√		
$x'y$	√	√	√	√

(*c*)

Fig. 15-37

15.72. Use a Karnaugh map to find a minimal sum for each Boolean expression:

(*a*) $E = xy + x'y + x'y'$. (*b*) $E = x + x'yz + xy'z'$.

15.73. Find a minimal sum for each Boolean expression:

(*a*) $E = y'z + y'z't' + z't$. (*b*) $E = y'zt + xzt' + xy'z'$.

15.74. Use Karnaugh maps to redesign each logic circuit L in Fig. 15-38 so that it becomes a minimal AND-OR circuit.

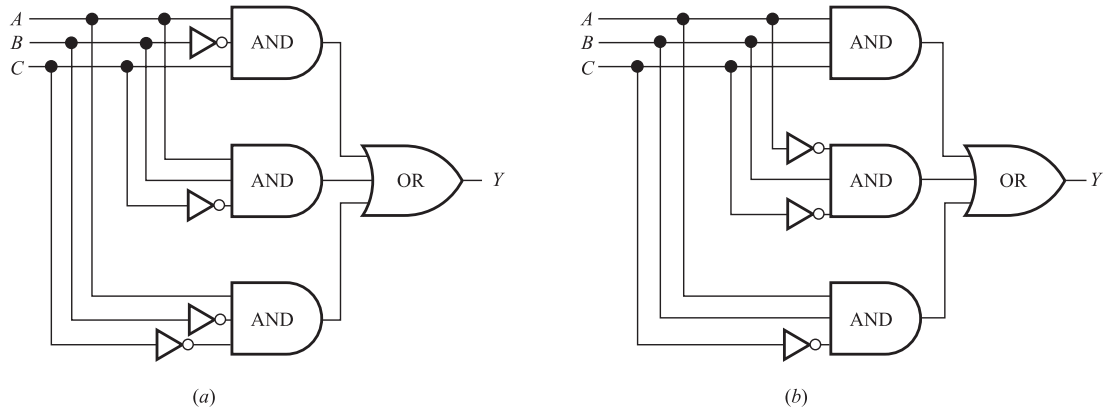


Fig. 15-38

15.75. Suppose three switches A, B, C are connected to the same hall light. At any moment a switch may be "up" denoted by 1 or "down" denoted by 0. A change in any switch will change the parity (odd or even) of the number of 1s. The switches will be able to control the light if it associates, say, an odd parity with the light being "on" (represented by 1), and an even parity with the light being "off" (represented by 0).

(*a*) Show that the following truth table satisfies these conditions:

$$T(A, B, C) = T(00001111, 00110011, 01010101) = 01101001$$

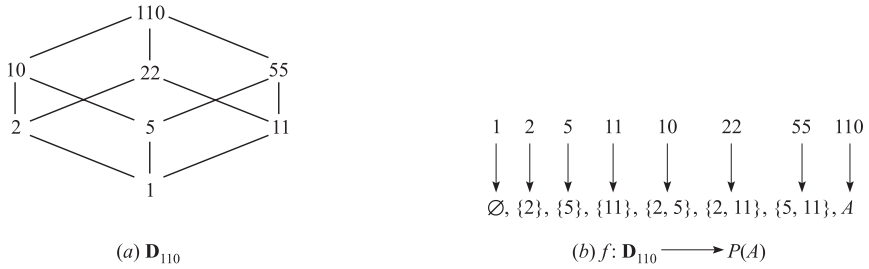
(*b*) Design a minimal AND-OR circuit L with the above truth table.

Answers to Supplementary Problems

15.43. (*a*) $a + a'b = a + b$.
(*b*) $a \cdot 0 + a \cdot 1 = a$.
(*c*) $ab + bc = (a + c)b$.

15.45. (*b*) $\mathbf{D}_{55}$; atoms 5 and 11. (*d*) $\mathbf{D}_{130}$; atoms 2, 5 and 13.

15.46. (*a*) There are eight elements 1, 2, 5, 10, 11, 22, 55, 110. See Fig. 15-39(*a*).
(*b*) There are five subalgebras: $\{1, 110\}$, $\{1, 2, 55, 110\}$, $\{1, 5, 22, 110\}$, $\{1, 10, 11, 110\}$, $\mathbf{D}_{110}$.
(*c*) There are 15 sublattices which include the above three subalgebras.
(*d*) $A = \{2, 5, 11\}$.
(*e*) See Fig. 15-39(*b*).



(*a*) $\mathbf{D}_{110}$ (*b*) f: $\mathbf{D}_{110} \longrightarrow P(A)$

Fig. 15-39

15.48. Maxterms: 30, 42, 70, 105

15.49. (*b*) *Hint*: Use duality.

15.53. (*a*) $xy'z$; (*b*) 0; (*c*) $xy'z't$; (*d*) 0.

15.54. (*a*) $E = xy' + xy'z = xy'z' + xy'z$.
(*b*) $E = xy + xz' = xyz + xyz' + xy'z'$.
(*c*) $E = xy' + y'z = xy'z + xy'z' + x'y'z$.

15.55. (*a*) $E = xyz' + x'y' = xyz' + x'y'z + x'y'z'$.
(*b*) $E = x'y' = x'y'z + x'y'z'$.
(*c*) $E = x'yz'$.

15.56. (*a*) $Q = xzt$. (*b*) $Q = xyt'$. (*c*) and (*d*) Does not exist.

15.57. (*a*) $E_L = 11$, $E_S = 3$. (*b*) $E_L = 11$, $E_S = 4$.

15.58. (*a*) $x'y$, $x'z'$, $y'z'$.
(*b*) xy', xzt', $y'zt'$, $x'z't$, $y'z't$.
(*c*) $xyzt$, $xz't'$, $y'z't'$, $x'y'z'$, $x'z't$.

15.59. (*a*) $E = x'y + x'z'$.
(*b*) $E = xy' + xzt' + x'z't + y'z't$.
(*c*) $E = xyzt + xz't' + x'y'z' + x'z't$.

15.60. (*a*) $Y = A'BC + A'C' + BC'$; (*b*) $A + B + C + A'BC + AB'C'$.

15.61. (*a*) $Y = (AB')' + (A' + B + C)' + AC$
(*b*) $Y = (A'BC)' + A'BC' + (AB'C)' + AB'C'$

15.62. See Fig. 15-40.

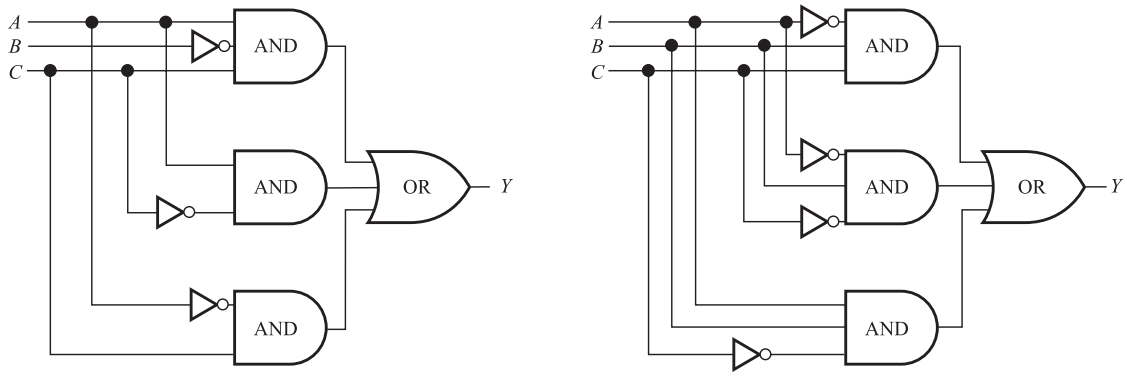


Fig. 15-40

15.63. (*a*) $Y = 100001$; (*b*) $Y = 00111000$; (*c*) $Y = 00110000$.

15.64. (*a*) $Y = 100111$; (*b*) $Y = 10100111$; (*c*) $Y = 11111101$.

15.65. (*a*) $A' = 00011000$; (*b*) $A' = 01110111$; (*c*) $A' = 00000111$.

15.66. (*a*) $2^n = 2^6 = 64$.
(*b*) $x_1 = 000 \cdots 00111 \cdot 11$ (32 zeros) (32 ones).
$x_2 = (00000000000000000111111111111111)^2$.
$x_3 = (0000000011111111)^4$.

15.67. (*a*) $T(E) = 01010011$; (*b*) $T(E) = 00111111$.

15.68. (*a*) $T(E) = 01000000$; (*b*) $T(E) = 10001010$.

15.69. Use truth tables for minterms in Example 15.13.
(*a*) $E = x'y'z' + xyz' + xyz'$.
(*b*) $E = xy'z' + xyz$.
(*c*) $E = x'yz' + xy'z'$.

15.70. (*a*) $E = xy' + x'y + yz = xy' + x'y + xz'$.
(*b*) $E = xy' + x'y + z$.
(*c*) $E = x' + z$.

15.71. (*a*) $E = x'y + zt' + xz't + xy'z = x'y + zt' + xz't + xy't$.
(*b*) $E = yz + yt' + zt' + xy'z'$.
(*c*) $E = x'y + yt + xy't' + x'zt = x'y + yt + xy't' + y'zt$.

15.72. (*a*) $E = x' + y$; (*b*) $E = xz' + yz$.

15.73. (*a*) $E = y' + z't$; (*b*) $E = xy' + zt' + y'zt$.

15.74. (*a*) See Fig. 15-41.

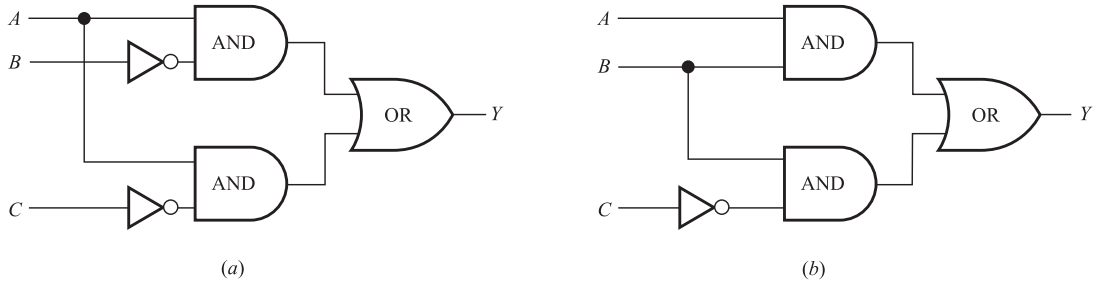


Fig. 15-41

15.75. (*b*) See Fig. 15-42.

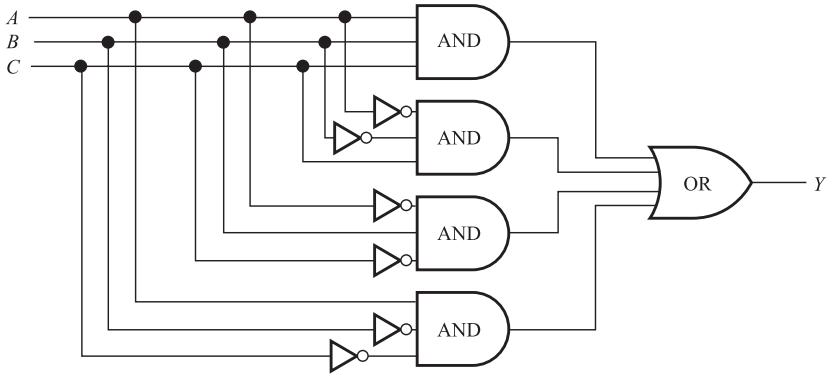


Fig. 15-42

© The McGraw–Hill Companies, 2004

Appendix A

Recurrence Relations

A.1 INTRODUCTION

Previously (Section 3.6) we discussed recursively defined functions such as:
(*a*) Factorial function, (*b*) Fibonacci sequence, (*c*) Ackermann function.

This Appendix A discusses certain kinds of recursively defined sequences $\{a_n\}$ and their solution. A sequence is simply a function whose domain is

$$\mathbf{N} = \{1, 2, 3, \ldots\} \text{ or } \mathbf{N}_0 = \mathbf{N} \cup \{0\}) = \{0, 1, 2, 3, \ldots\}$$

We begin with some examples.

EXAMPLE A.1 Consider the following sequence which begins with the number 3 and each of the following terms is obtained by multiplying the previous term by 2:

$$3, 6, 12, 24, 48, \ldots$$

It can be defined recursively by:

$$a_0 = 3, a_k = 2a_{k-1} \text{ for } k \geq 1, \text{ or } a_0 = 3, a_{k+1} = 2a_k \text{ for } k \geq 0.$$

[The second definition may be obtained from the first by setting $k = k + 1$.] Clearly, the formula $a_n = 3(2^n)$ gives us the nth term of the sequence without calculating any previous term. The following remarks are in order.

(1) The equation $a_k = 2a_{k-1}$ or, equivalently, $a_{k+1} = 2a_k$, where one term of the sequence is defined in terms of previous terms of the sequence, is called a *recurrence relation*.
(2) The equation $a_0 = 3$, which gives a specific value to one of the terms, is called an *initial condition*.
(3) The function $a_n = 3(2^n)$, which gives a formula for a_n as a function of n, not of previous terms, is called a *solution* of the recurrence relation.
(4) There may be many sequences which satisfy a given recurrence relation. For example:
1, 2, 4, 8, 16, . . . and 7, 14, 28, 56, 112, . . .
are each solutions of the recurrence relation $a_k = 2a_{k-1}$. All such solutions form the so-called *general solution* of the recurrence relation.
(5) On the other hand, there may be only a unique solution to a recurrence relation which also satisfies given initial conditions. For example, the initial condition $a_0 = 3$ uniquely yields the solution 3, 6, 12, 24, . . . of the recurrence relation $a_k = 2a_{k-1}$.

This Appendix shows us how to solve certain recurrence relations. First we give two important sequences the reader may have previously studied.

EXAMPLE A.2

(*a*) *Arithmetic Progression*

An arithmetic progression is a sequence of the form

$$a, a + d, a + 2d, a + 3d, \ldots$$

That is, the sequence begins with the number a and each successive term is obtained from the previous term by adding d (the common difference between any two terms). For example:

(i) $a = 5, d = 3 : 5, 8, 9, 11, \ldots$
(ii) $a = 2, d = 5 : 2, 7, 12, 17, \ldots$
(iii) $a = 1, d = 0 : 1, 1, 1, 1, 1, \ldots$

We note that the general arithmetic progression may be defined recursively by:

$$a_1 = a \text{ and } a_{k+1} = a_k + d \text{ for } k \geq 1$$

where the solution is $a_n = a + (n-1)d$.

(*b*) *Geometric Progression*

A geometric progression is a sequence of the form

$$a, ar, ar^2, ar^3, \ldots$$

That is, the sequence begins with the number a and each successive term is obtained from the previous term by multiplying by r (the common ratio between any two terms). For example:

(i) $a = 1, r = 3 : 1, 3, 9, 27, 81, \ldots$

(ii) $a = 5, r = 2 : 5, 10, 20, 40, \ldots$

(iii) $a = 1, r = \frac{1}{2} : 1, \frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \ldots$

We note that the general geometric progression may be defined recursively by:

$$a_1 = a \text{ and } a_{k+1} = ra_k \text{ for } k \geq 1$$

where the solution is $a_{n+1} = ar^n$.

A.2 LINEAR RECURRENCE RELATIONS WITH CONSTANT COEFFICIENTS

A *recurrence relation* of *order* k is a function of the form

$$a_n = \Phi(a_{n-1}, a_{n-2}, \ldots, a_{n-k}, n)$$

that is, where the nth term a_n of a sequence is a function of the preceding k terms $a_{n-1}, a_{n-2}, \ldots, a_{n-k}$ (and possibly n). In particular, a *linear* k*th-order recurrence relation with constant coefficients* is a recurrence relation of the form

$$a_n = C_1 a_{n-1} + C_2 a_{n-2} + \ldots + C_k a_{n-k} + f(n)$$

where $C_1, C_2, \ldots, C_k$ are constants with $C_k \neq 0$, and $f(n)$ is a function of n. The meaning of the names linear and constant coefficients follow:

linear: There are no powers or products of the $a_j's$.

constant coefficients: The $C_1, C_2, \ldots, C_k$ are constants (do not depend on n).

If $f(n) = 0$, then the relation is also said to be *homogeneous*.

Clearly, we can uniquely solve for a_n if we know the values of $a_{n-1}, a_{n-2}, \ldots, a_{n-k}$. Accordingly, by mathematical induction, there is a unique sequence satisfying the recurrence relation if we are given *initial values* for the first k elements of the sequence.

EXAMPLE A.3 Consider each of the following recurrence relations:

(*a*) $a_n = 5a_{n-1} - 4a_{n-2} + n^2$

This is a second-order recurrence relation with constant coefficients. It is nonhomogeneous because of the n^2. Suppose we are given the initial conditions $a_1 = 1, a_2 = 2$. Then we can find sequentially the next few elements of the sequence:

$$a_3 = 5(2) - 4(1) + 3^2 = 15, a_4 = 5(15) - 4(2) + 4^2 = 83$$

(*b*) $a_n = 2a_{n-1}a_{n-2} + n^2$

The product $a_{n-1}a_{n-2}$ means the recurrence relation is not linear. Given initial conditions $a_1 = 1, a_2 = 2$, we can still find the next few elements of the sequence:

$$a_3 = 2(2)(1) + 3^2 = 13, a_4 = 2(13)(2) + 4^2 = 68$$

(*c*) $a_n = na_{n-1} + 3a_{n-2}$

This is a homogeneous linear second-order recurrence relation but it does not have constant coefficients because the coefficient of a_{n-1} is n, not a constant. Given initial conditions $a_1 = 1, a_2 = 2$, the next few elements of the sequence follow:

$$a_3 = 3(2) + 3(1) = 9, a_4 = 4(9) + 3(2) = 42$$

(*d*) $a_n = 2a_{n-1} + 5a_{n-2} - 6a_{n-3}$

This is a homogeneous linear third-order recurrence relation with constant coefficients. Thus we need three, not two, initial conditions to yield a unique solution of the recurrence relation. Suppose we are given the initial conditions $a_1 = 1, a_2 = 2, a_3 = 1$. Then the next few elements of the sequence follow:

$$a_4 = 2(1) + 5(2) - 6(1) = 6, a_5 = 2(2) + 5(1) - 6(6) = -37,$$
$$a_6 = 2(1) + 5(6) - 6(-37) = 254$$

This appendix will investigate the solutions of homogeneous linear recurrence relations with constant coefficients. The theory of nonhomogeneous recurrence relations and recurrence relations without constant coefficients lie beyond the scope of this text.

For computational convenience, most of our sequences will begin with a_0 rather than a_1. The theory is not affected at all.

A.3 SOLVING SECOND-ORDER HOMOGENEOUS LINEAR RECURRRENCE RELATIONS

Consider a homogeneous second-order recurrence relation with constant coefficients which has the form

$$a_n = sa_{n-1} + ta_{n-2} \text{ or } a_n - sa_{n-1} - ta_{n-2} = 0$$

where s and t are constants with $t \neq 0$. We associate the following quadratic polynomial with the above recurrence relation:

$$\Delta(x) = x^2 - sx - t$$

This polynomial $\Delta(x)$ is called the *characteristic polynomial* of the recurrence relation, and the roots of $\Delta(x)$ are called its *characteristic roots*.

The following theorems apply.

Theorem A.1: Suppose the characteristic polynomial

$$\Delta(x) = x^2 - sx - t \text{ of the recurrence relation}$$
$$a_n = sa_{n-1} + ta_{n-2}$$

has distinct real roots r_1 and r_2. Then the general solution of the recurrence relation is

$$a_n = c_1 r_1^n + c_2 r_2^n$$

where c_1 and c_2 are arbitrary constants.

We emphasize that the constants c_1 and c_2 may be uniquely computed using initial conditions. We note that the theorem is true even when the roots are not real. Such cases lie beyond the scope of this text.

EXAMPLE A.4 Consider the following homogeneous recurrence relation:

$$a_n = 2a_{n-1} + 3a_{n-2}$$

The general solution is obtained by finding the characteristic polynomial $\Delta(x)$ and its roots r_1 and r_2:

$$\Delta(x) = x^2 - 2x - 3 = (x - 3)(x + 1); \text{ roots } r_1 = 3, r_2 = -1$$

Since the roots are distinct, we can use Theorem A.1 to obtain the general solution:

$$a_n = c_1 3^n + c_2(-1)^n$$

Thus any values for c_1 and c_2 will give a solution to the recurrence relation.

Suppose we are also given the initial conditions $a_0 = 1, a_1 = 2$. Using the recurrence relation we can compute the next few terms of the sequence:

$$1, 2, 8, 28, 100, 356, 1268, 3516, \ldots$$

The unique solution is obtained by finding c_1 and c_2 using the initial conditions. Specifically:

For $n = 0, a_0 = 1 : c_1 3^0 + c_2(-1)^0 = 1$ or $c_1 + c_2 = 1$.
For $n = 1, a_1 = 2 : c_1 3^1 + c_2(-1)^1 = 2$ or $3c_1 - c_2 = 2$.

Solving the system of the two equations in c_1 and c_2 yields:

$$c_1 = \frac{3}{4}, c_2 = \frac{1}{4}.$$

Thus the following is the unique solution of the given recurrence relation with initial conditions $a_0 = 1, a_1 = 2$:

$$a_n = \frac{3}{4}3^n + \frac{1}{4}(-1)^n = \frac{3^{n+1} + (-1)^n}{4}$$

EXAMPLE A.5 Consider the celebrated Fibonacci sequence:

$$a_n = a_{n-1} + a_{n-2}, \text{ with } a_0 = 0, a_1 = 1$$

The first 10 terms of the sequence follow:

$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, \ldots$$

Sometimes the Fibonacci sequence is defined using the initial conditions $a_0 = 1, a_1 = 1$ or the initial conditions $a_1 = 1, a_2 = 2$. We use $a_0 = 0, a_1 = 1$ for computational convenience. (All three initial conditions yield the same sequence after the pair of terms 1, 2.)

Observe that the Fibonacci sequence is a homogeneous linear second-order recurrence relation, so it can be solved using Theorem A.1. Its characteristic polynomial follows:

$$\Delta(x) = x^2 - x - 1$$

Using the quadratic formula, we obtain the roots:

$$r_1 = \frac{1 + \sqrt{5}}{2}, \quad r_2 = \frac{1 - \sqrt{5}}{2}$$

By Theorem A.1, we obtain the general solution:

$$a_n = c_1\left(\frac{1 + \sqrt{5}}{2}\right)^n + c_2\left(\frac{1 - \sqrt{5}}{2}\right)^n$$

The initial conditions yield the following system of two linear equations in c_1 and c_2:

For $n = 0, a_0 = 0$: $\quad 0 = c_1 + c_2$

For $n = 1, a_0 = 1$: $\quad 1 = c_1\left(\frac{1 + \sqrt{5}}{2}\right) + c_2\left(\frac{1 - \sqrt{5}}{2}\right)$

The solution of the system follows:

$$c_1 = \frac{1}{\sqrt{5}}, c_2 = -\frac{1}{\sqrt{5}}$$

Accordingly, the following is the solution of the Fibonacci recurrence relation:

$$a_n = \frac{1}{\sqrt{5}}\left(\frac{1 + \sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1 - \sqrt{5}}{2}\right)^n$$

One can show that the absolute value of the above second term for a_n is always less than $1/2$. Thus a_n is also the closest integer to the number

$$\frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n \approx (0.4472)(1.6180)^n$$

The approximate first few values of the above expression follow:

$$0.4472, 0.7236, 1.1708, 1.8944, 3.0653, 4.99597, 8.0249, 12.9846, 21.0092$$

Suppose the roots of the characteristic polynomial are not distinct. Then we have the following result.

Theorem A.2: Suppose the characteristic polynomial $\Delta(x) = x^2 - sx - t$ of the recurrence relation

$$a_n = sa_{n-1} + ta_{n-2}$$

has only one root r_0. Then the solution of the recurrence relation is

$$a_n = c_1 r_0^n + c_2 n r_0^n$$

where c_1 and c_2 are arbitrary constants.

Again we note that the constants c_1 and c_2 may be uniquely computed using initial conditions.

EXAMPLE A.6 Consider the following homogeneous recurrence relation:

$$a_n = 6a_{n-1} - 9a_{n-2}$$

The characteristic polynomial $\Delta(x)$ follows:

$$\Delta(x) = x^2 - 6x + 9 = (x-3)^2$$

Thus $\Delta(x)$ has only the one root $r_0 = 3$. Now we use Theorem A.2 to obtain the following solution of the recurrence relation:

$$a_n = c_1 3^n + c_2 n 3^n$$

Thus any values for c_1 and c_2 will give a solution to the recurrence relation.

Suppose we are also given the initial conditions $a_1 = 3, a_2 = 27$. Using the recurrence relation we can compute the next few terms of the sequence:

$$3, 27, 135, 567, 2187, 8109, \ldots$$

The unique solution is obtained by finding c_1 and c_2 using the initial conditions. Specifically:

For $n = 1, a_1 = 3$: $\quad 3 = c_1 3^1 + c_2(1)(3)^1$ or $3c_1 + 3c_2 = 3$.
For $n = 2, a_2 = 27$: $\quad 27 = c_1 3^2 + c_2(2)(3)^1$ or $9c_1 + 18c_2 = 27$.

Solving the system of the two equations in c_1 and c_2 yields:

$$c_1 = -1, c_2 = 2$$

Thus the following is the unique solution of the given recurrence relation with initial conditions $a_1 = 3, a_2 = 27$:

$$a_n = -3^n + 2n3^n = 3^n(2n-1)$$

A.4 SOLVING GENERAL HOMOGENEOUS LINEAR RECURRENCE RELATIONS

Consider now a general linear homogeneous kth-order recurrence relation with constant coefficients which has the form

$$a_n = C_1 a_{n-1} + C_2 a_{n-2} + C_3 a_{n-3} + \ldots + C_k a_{n-k} = \sum_{i=1}^{k} C_i a_{n-i} \tag{A.1}$$

where $C_1, C_2, \ldots, C_k$ are constants with $C_k \neq 0$. The *characteristic polynomial* $\Delta(x)$ of the recurrence relation (A.1) follows:

$$\Delta(x) = x^k - C_1 x^{k-1} - C_2 x^{k-2} - C_3 x^{k-3} - \ldots - C_k = x^k - \sum_{i=1}^{k} C_i x^{k-i}$$

The roots of $\Delta(x)$ are called the *characteristic roots* of the recurrence relation.

The following remarks are in order.

Remark 1: If $p(n)$ and $q(n)$ are solutions of (A.1), then any linear combination

$$c_1 p(n) + c_2 q(n)$$

of $p(n)$ and $q(n)$ is also a solution. (This is not true if the recurrence relation is nonhomogeneous.)

Remark 2: If r is a root of multiplicity m of the characteristic polynomial $\Delta(x)$ of (A.1), then each of the following

$$r^n, nr^n, n^2r^n, \ldots, n^{m-1}r^n$$

is a solution of (A.1). Thus any linear combination

$$\begin{aligned} &c_1 r^n + c_2 nr^n + c_3 n^2 r^n + \ldots + c_m n^{m-1} r^n \\ &= (c_1 + c_2 n + c_3 n^2 + \ldots + c_m n^{m-1}) r^n \end{aligned}$$

is also a solution.

EXAMPLE A.7 Consider the following third-order homogeneous recurrence relation:

$$a_n = 11a_{n-1} - 39a_{n-2} + 45a_{n-3}$$

The characteristic polynomial $\Delta(x)$ of the recurrence relation is

$$\Delta(x) = x^3 - 11x^2 + 39x - 45 = (x-3)^2(x-5)$$

There are two roots, $r_1 = 3$ of multiplicity 2 and $r_2 = 5$ of multiplicity 1. Thus, by the above remarks, the general solution of the recurrence relation is

$$a_n = c_1(3^n) + c_2 n(3^n) + c_3(5^n) = (c_1 + c_2 n)(3^n) + c_3(5^n)$$

Suppose we are given the initial conditions $a_0 = 5, a_1 = 11, a_2 = 25$. The next few terms of the sequence follow:

$$5, 11, 25, 71, 301, 1667, \ldots$$

The unique solution of the system is obtained by finding the values of c_1, c_2, c_3 using the initial conditions. Specifically:

For $n = 1, a_0 = 5$: $\quad c_1 + c_3 = 5$
For $n = 1, a_1 = 11$: $\quad 3c_1 + 3c_2 + 5c_3 = 11$
For $n = 2, a_2 = 25$: $\quad 9c_1 + 18c_2 + 25c_3 = 25$

Solving the system of the three equations in c_1, c_2, c_3 yields:

$$c_1 = 4, c_2 = -2, c_3 = 1$$

Thus the following is the unique solution of the given recurrence relation with the given initial conditions:

$$a_n = (4 - 2n)(3^n) + 5^n$$

EXAMPLE A.8 Consider the following third-order homogeneous recurrence relation:

$$a_n = 6a_{n-1} - 12a_{n-2} + 8a_{n-3}$$

The characteristic polynomial $\Delta(x)$ of the recurrence relation is

$$\Delta(x) = x^3 - 6x^2 + 12x - 8 = (x-2)^3$$

Thus $\Delta(x)$ has only the one root $r_0 = 2$ which has multiplicity 3. Thus the general solution of the recurrence relation is

$$a_n = c_1(2^n) + c_2 n(2^n) + c_3 n^2(2^n) = (c_1 + c_2 n + c_3 n^2)2^n$$

Suppose we are given the initial conditions $a_0 = 3, a_1 = 4, a_2 = 12$. Then we can find values for c_1, c_2, c_3. Specifically:

For $n = 0, a_0 = 3$: $c_1 = 3$
For $n = 1, a_1 = 4$: $2c_1 + 2c_2 + 2c_3 = 4$
For $n = 2, a_2 = 12$: $4c_1 + 8c_2 + 16c_3 = 12$

Solving the system of the three equations in c_1, c_2, c_3 yields:

$$c_1 = 3, c_2 = -2, c_3 = 1$$

Thus the following is the unique solution of the given recurrence relation:

$$a_n = (3 - 2n + n^2)(2^n)$$

Remark: Finding the roots of the characteristic polynomial $\Delta(x)$ is an important step in solving recurrence relations. Generally speaking, this may be difficult when the order k is greater than 2. (Example 12.17 indicates one way to find the roots of some polynomials of degree 3 or more.)

Supplementary Problems

LINEAR HOMOGENEOUS RECURRENCE RELATIONS WITH CONSTANT COEFFICIENTS

A.1. Find the characteristic polynomial $\Delta(x)$ and the general solution to each recurrence relation:

(*a*) $a_n = 3a_{n-1} + 10a_{n-2}$ (*c*) $a_n = 3a_{n-1} - 2a_{n-2}$ (*e*) $a_n = 3a_{n-1} - a_{n-2}$
(*b*) $a_n = 4a_{n-1} + 21a_{n-2}$ (*d*) $a_n = 5a_{n-1} - 6a_{n-2}$ (*f*) $a_n = 5a_{n-1} - 3a_{n-2}$

A.2. Given the following initial conditions, find the unique solution to each recurrence relation in Problem A.1:

(*a*) $a_0 = 5, a_1 = 11$ (*c*) $a_0 = 5, a_1 = 8$ (*e*) $a_0 = 0, a_1 = 1$
(*b*) $a_0 = 9, a_1 = 13$ (*d*) $a_1 = 2, a_2 = -8$ (*f*) $a_0 = 0, a_1 = 1$

A.3. Find the characteristic polynomial $\Delta(x)$ and the general solution to each recurrence relation:

(*a*) $a_n = 6a_{n-1}$ (*b*) $a_n = 7a_{n-1}$ (*c*) $a_n = 4a_{n-1} - 4a_{n-2}$ (*d*) $a_n = 10a_{n-1} - 25a_{n-2}$

A.4. Given the following initial conditions, find the unique solution to each recurrence relation in Problem A.3:

(*a*) $a_0 = 5$ (*b*) $a_1 = 5$ (*c*) $a_0 = 1, a_1 = 8$ (*d*) $a_0 = 2, a_1 = 15$

A.5. Find the characteristic polynomial $\Delta(x)$ and the general solution to each recurrence relation:

(*a*) $a_n = 6a_{n-1} - 11a_{n-2} + 6a_{n-3}$ (*b*) $a_n = 11a_{n-1} - 39a_{n-2} + 45a_{n-3}$

A.6. Find the unique solution to each recurrence relation and initial conditions:

(*a*) $a_n = 10a_{n-1} - 32a_{n-2} + 32a_{n-3}$ with $a_0 = 5, a_1 = 18, a_2 = 78$
(*b*) $a_n = 9a_{n-1} - 27a_{n-2} + 27a_{n-3}$ with $a_0 = 5, a_1 = 24, a_2 = 117$

MISCELLANEOUS PROBLEMS

A.7. Consider the following second-order recurrence relation and its characteristic polynomial $\Delta(x)$:

$$a_n = sa_{n-1} + ta_{n-2}, \Delta(x) = x^2 - sx - t \qquad (*)$$

(*a*) Suppose $p(n)$ and $q(n)$ are solutions of $(*)$. Show that $c_1p(n) + c_2q(n)$, for any constants c_1 and c_2, is also a solution of $(*)$.

(*b*) Suppose r is a root of $\Delta(x)$. Show that $a_n = r^n$ is a solution of $(*)$.

A.8. Suppose r is a double root of $\Delta(x) = x^2 - sx - t$.

(*a*) Show that $s = 2r$ and $t = -r^2$.

(*b*) Show that $a_n = nr^n$ is also a root of $(*)$.

A.9. Repeat Problem A.6 for any linear kth-order homogeneous recurrence relation with constant coefficients which has the form

$$a_n = C_1a_{n-1} + C_2a_{n-2} + \ldots + C_ka_{n-k} = \sum_{i=1}^{k} C_ia_{n-i}$$

with characteristic polynomial $\Delta(x) = x^k - \sum C_ix^{k-i}$.

Answers to Supplementary Problems

A.1. (*a*) $\Delta(x) = x^2 - 3x - 10, a_n = c_1(5^n) + c_2(-2)^n$
(*b*) $\Delta(x) = x^2 - 4x - 21, a_n = c_1(7^n) + c_2(-3)^n$
(*c*) $\Delta(x) = x^2 - 3x + 2, a_n = c_1 + c_2(2^n)$
(*d*) $\Delta(x) = x^2 - 5x + 6, a_n = c_1(2^n) + c_2(3^n)$
(*e*) $\Delta(x) = x^2 - 3x + 1, a_n = c_1[(3 + \sqrt{5})/2]^n + c_2[(3 - \sqrt{5})/2]^n$
(*f*) $\Delta(x) = x^2 - 5x + 3, a_n = c_1[(5 + \sqrt{13})/2]^n + c_2[(5 - \sqrt{13})/2]^n$

A.2. (*a*) $a_n = 3(5^n) + 2(-2)^n$ (*b*) $a_n = 4(7^n) + 5(-3)^n$
(*c*) $a_n = 2 + 3(2^n)$ (*d*) $a_n = 7(2^n) - 4(3^n)$

(*e*) $$a_n = \frac{1}{\sqrt{5}}\left(\frac{3+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{3-\sqrt{5}}{2}\right)^n$$

(*f*) $$a_n = \frac{1}{\sqrt{13}}\left(\frac{5+\sqrt{13}}{2}\right)^n - \frac{1}{\sqrt{13}}\left(\frac{5-\sqrt{13}}{2}\right)^n$$

A.3. (*a*) $\Delta(x) = x - 6, a_n = c_1(6^n)$
(*b*) $\Delta(x) = x - 7, a_n = c_1(7^n)$
(*c*) $\Delta(x) = x^2 - 4x + 4, a_n = c_1(2^n) + c_2n(2^n) = (c_1 + nc_2)2^n$
(*d*) $\Delta(x) = x^2 - 10x + 25, a_n = c_1(5^n) + c_2n(5^n) = (c_1 + nc_2)5^n$

A.4. (*a*) $a_n = 5(6^n)$ (*c*) $a_n = (2^n) + 3n(2^n) = (1 + 3n)2^n$
(*b*) $a_n = 5(7^{n-1})$ (*d*) $a_n = 2(5^n) + n(5^n) = (2 + n)5^n$

A.5. (*a*) $\Delta(x) = x^3 - 5x^2 + 11x - 6, a_n = c_1 + c_2(2^n) + c_3(3^n)$
(*b*) $\Delta(x) = x^3 - 11x^2 + 39x - 45, a_n = c_1(3^n) + c_2n(3^n) + c_3(5^n)$

A.6. (*a*) $a_n = 2(4^n) + n(4^n) + 3(2^n)$
(*b*) $a_n = 5(3^n) + 2n(3^n) + n^2(3^n) = (5 + 2n + n^2)3^n$

A.7. (*a*) We are given that $p(n)$ and $q(n)$ are solutions of $(*)$; hence:

$$p(n) = sp(n-1) + tp(n-2) \quad \text{and} \quad q(n) = sq(n-1) + tq(n-2)$$

Then

$$\begin{aligned} c_1p(n) + c_2q(n) &= c_1[sp(n-1) + tp(n-2)] + c_2[sq(n-1) + tq(n-2)] \\ &= s[c_1p(n-1) + c_2q(n-1)] + t[c_1p(n-2) + c_2q(n-2)] \end{aligned}$$

Hence $c_1p(n) + c_2q(n)$ is also a solution of $(*)$.

(*b*) We are given that r is a root of $\Delta(x)$. Hence

$$r^2 - sr - t = 0 \quad \text{and} \quad r^2 = sr + t$$

Let $a_n = r^n$. Then

$$\begin{aligned} sa_{n-1} + ta_{n-2} &= sr^{n-1} + tr^{n-2} = (sr + t)r^{n-2} \\ &= r^2(r^{n-2}) = r^n = a_n \end{aligned}$$

Thus $a_n = r^n$ is a solution of $(*)$.

A.8. (*a*) We are given that r is a double root of $\Delta(x)$. Hence

$$\Delta(x) = (x - r)^2 = x^2 - 2rx + 2^2$$

But $\Delta(x) = x^2 - sx - t$. Hence $s = 2r$ and $t = -r^2$.

(*b*) Let $a_n = nr^n$. Then

$$\begin{aligned} sa_{n-1} + ta_{n-2} &= s(n-1)r^{n-1} + t(n-2)r^{n-2} \\ &= 2r(n-1)r^{n-1} - r^2(n-2)r^{n-2} = 2(n-1)r^n - (n-2)r^n \\ &= r^n[2(n-1) - (n-2)] = r^n[2n - 2 - n + 2] = nr^n = a_n \end{aligned}$$

Thus $a_n = r^n$ is a solution of $(*)$.

© The McGraw–Hill Companies, 2004

Index

Abelian group, 371
Absolute value, 54, 316
Absorption law, 451
Abstraction, Principle of, 2
Accepting (yes) states, 408
Ackermann function, 61
Acyclic, 250
Address, 237
Adjacency:
  matrix, 205, 239
  structure (AS), 206, 245
Adjacent:
  fundamental products, 492
  regions, 204
  vertices, 190, 233
Aleph-naught, $\aleph_0$, 61
Algebra:
  Boolean, 477
  Fundamental Theorem of, 382
Algebra of:
  matrices, 109
  propositions, 83
  sets, 7, 17
Algebraic expression, 277
Algorithms, 62–66
  complexity of, 64
  division, 318
  Euclidean, 63, 322, 380
Alphabet, 405
Ancestor, 278
AND gate, 487
AND-OR circuit, 488
Antisymmetric relation, 33
Apple-Haken Theorem, 204
Arcs, 233
Arguments, 4, 23, 85
Array, 102
Associates, 379
Associative operations, 365
Atoms, 454
Augmented matrix, 108
AUT(·)(automorphisms), 372
Automaton, 408
  linear bounded, 415
  pushdown, 415
Automorphism, 372
Average case, 64

Backus-Naur form, 415
Base value, 59
Basic rectangle, 494, 496
  maximal, 495
Bernoulli trials, 158
BFS (breadth-first-search), 209, 247
Biconditional statement, 84
Big O notation, 65
Bijective function, 53
Binary:
  addition, 417
  digit, 117, 477
  operation, 364
  relation, 28
  search, 66
Binary search tree, 284
  complexity of algorithms, 286
Binary tree, 276
  complete, 277
  extended, 279
  similar, 277
Binomial:
  coefficients, 134
  distribution, 159
Bipartite graphs, 198
Bits, 477
Boolean:
  algebra, 477–486
  expression, 481
    minimal, 483
  function, 491
  matrix, 117, 239
  ring, 401
  subalgebra, 478
Bounded:
  lattices, 453
  sets, 447
Breadth-first-search, 209, 247
Bridge (in a graph), 194
Bubble sort, 66

C, complex numbers, 2
$C(n, r)$ (combinations), 138
Cancelation law, 367
  for congruences, 327
Cantor, 61
  theorem, 62, 74

Cardinal numbers, 61–62, 70
  inequalities, 62
Carroll, Lewis, 4
Cartesian product, 27
Ceiling function, 54
Chain, 443
Children, 278, 294
Chinese Remainder Theorem, 332, 357
Choice, Axiom of, 451
Chromatic number, 203
Circuit, 193, 235
  Hamiltonian, 195
  logic, 486
Classes of sets, 10, 18
  residue, 326
Closed path, 193, 235
Closure, Kleene, 444
Closure of relations, 34, 42
  transitive, 242
Code, 293
  Huffman, 293
Codomain, 50
Colored:
  graphs, 203
  maps, 223
Column, 104
Combinations, 137, 145
Commutative operation, 365
  group, 371
Comparable elements, 443
Complement:
  in a Boolean algebra, 477
  in a lattice, 454
  of a set, 6
Complemented lattice, 454
Complete:
  binary tree, 278
  graph, 197
  sum-of-products form, 483
Complex numbers **C**, 2
Complexity of algorithms, 64
  in a binary search tree, 286
  in a heap, 286
Composition:
  of functions, 52
  of relations, 32
Compound statement, 78
Computable function, 422–424, 433
Computer representation:
  of binary trees, 280
  of directed graphs, 239
  of graphs, 205
Concatenation, 405
Conclusion, 85
Conditional probability, 155, 168
Conditional statement, 84
Congruence relation, 325, 345
  arithmetic, 326
  equations, 329
Conjunction, 79
Connected graph, 193
  components, 193
  map, 201
  strongly, 235
  unilaterally, 235
  weakly, 235
Consensus, 484
  method, 485
Consistent enumeration, 446, 459
Context-free grammar, 414
Context-sensitive grammar, 413
Contradiction, 82
Contrapositive statement, 95
Converse statement, 95
Coprime, 323
Coset, 372
Countable set, 62
Counterexample, 91
Counting principle, 9, 133
Cover, minimal, 495
Cross partition, 23
Cutpoint, 194
Cycle, 193, 235
  Hamiltonian, 195
Cycle-free, 199
Cyclic group, 374

$\mathbf{D}_m$, 478
$d(u, v)$ (distance), 194
Dag (directed acyclic graph), 250
Degree:
  of a polynomial, 378
  of a region, 201
  of a vertex, 191, 234
DeMorgan's law, 8, 11, 90, 479
Dense graph, 205
Denumerable set, 62
Depth:
  of a binary tree, 278
  of recursion, 60
Depth-first-search, 209, 247
Derivation tree, 414
Descendant, 278
Detachment, Law of, 85
Determinants, 110–112
Diagonal of a matrix, 108
Diagram:
  Hasse, 444
  state, 409, 416
  Venn, 3, 14
Diameter of a graph, 194
Dictionary order, 444
Digraph (directed graph), 233-235
  matrix of, 239

Dihedral group, 400
Direct product of groups, 401
Directed graph, 233–235
  of a relation, 30
Disjoint sets, 5
Disjunction (or), 79
Disjunctive normal form, 483
Distance between vertices, 194
Distribution, 159
  binomial, 162
Distributive lattice, 454
Divisibility, 378
  of integers, 319, 341
  of polynomials, 379
Division algorithm, 318, 338
Domain:
  of a function, 50
  of a relation, 28
Domain (integral), 376
Dot product, 103
Dual:
  map, 204
  order, 442
Duality:
  in a Boolean algebra, 478
  in a lattice, 451
  Principle of, 9, 17, 451, 478

$E(G)$ (edges in a graph), 190
Echelon matrix, 113, 125
Edge, 190, 233
  parallel, 234
  file, 206, 246
Element of a set, 1
Elimination, Gaussian, 112, 125
Empty:
  relation, 29
  set $\varnothing$, 2
  word, 405
Endpoints, 190
Equality:
  of functions, 50
  of matrices, 104
  of sets, 1
Equality relation, 29
Equipotent, 61
Equiprobable space, 154, 164
Equivalence:
  class, 36
  relation, 35, 44, 47
Equivalence, logical, 83
Euclidean algorithm, 63, 322, 380
Euler:
  formula, 201, 322
  phi function, 328, 347
Eulerian graph, 195
  trail, 195
Event (probability), 152
  elementary, 152
  independent, 156, 170
Existential quantifier, 88
Expectation, 64, 160, 174
Exponential function, 55
Expression, 419
  algebraic, 277
  regular, 407
Extended binary tree, 279
Extension, Principle of, 1
External node, 279, 290

Factor Theorem, 380
Factorial, 59, 134
Fibonacci sequence, 60
Field, 376, 393
File, 246
  edge, 206
  vertex, 206
Finite:
  graph, 191
  probability space, 153
  set, 9, 16
  state automaton (FSA), 408, 427
  state machine, 416
First element, 446
Floor function, 54
Forest, 198, 295
Four Color Theorem, 204
Free semigroup, 367, 406
  order, 444
Function, 60–71
  computable, 422–424, 433
  next-state, 408
  polynomial, 52
  rate of growth, 65
  recursively defined, 59
Fundamental product, 7, 481
  adjacent, 492

Gates, logic, 486
Gaussian elimination, 112
$\gcd(a, b)$ (greatest common divisor), 321
General tree, 294–295
Generators of a group, 374
Gödel number, 418
Grammar, 411, 429
  types of, 413
Graph, 188
  adjacency structure (AS), 206, 245
  bipartite, 198
  complete, 197
  connected, 193
  directed, 233–235
  of a function, 51
  labeled, 196, 233

Graph (*Cont.*):
matrix of, 205
planar, 200–203
regular, 197
of a relation, 29
weighted, 196
Greatest common divisor, 63, 321
Group, 371, 386
cyclic, 374
homomorphisms, 375
quotient, 373
symmetric, 372
Growth of functions, rate of, 65

Hamiltonian graph, 195
cycle, 195
Hasse diagram, 444
Heap, 287–290
Homeomorphic graphs, 192
Homomorphism:
of groups, 375
of rings, 378
of semigroups, 369
Horner's method, 63
Huffman's algorithm, 291
code, 293

I_n (identity matrix), 108
Ideal, 377
Idempotent laws, 8, 451
Identity:
element, 366
function, 51
matrix, 108
relation, 29
Image of a function, 50, 375
Implication, logical, 87
Impossible event, 152
Incidence, 190
Inclusion map, 51
Inclusion-Exclusion Principle, 139
Indegree, 234
Independent:
events, 156, 170
repeated trials, 151, 171
Index of a subgroup, 373
Indexed sets, 58
Induction, mathematical, 12, 317, 450
transfinite, 450
Inequalities, 315, 334
Infimum (inf), 447, 460
Infinite set, 61
Initial state, 408, 419
Injective function, 53
Inner product, 103
Inorder traversal, 282
Input (in a Turing machine), 421

Integer value, 54
Integers, 315–323
modulo m, 327, 374, 376
Integral domain, 376
Internal nodes, 277, 290
Intersection of sets, 5, 11
Inverse:
element, 366
function, 53
matrix, 109, 116
order, 442
relation, 29
Invertible:
functions, 53, 68
matrices, 109
Irreducible element:
in a lattice, 454
in a ring, 378
Irredundant decompositions, 454
Isolated vertex, 191
Isomorphic:
Boolean algebras, 478
graphs, 192
groups, 375
lattices, 453
ordered sets, 449
rings, 378
semigroups, 309

Join, 451
irreducible, 454

$\mathbf{K}_n$ (complete graph), 197
$\mathbf{K}_{m,n}$ (complete bipartite graph), 198
Karnaugh maps, 492–497
Kernel (Ker), 375
Kleene, 410
closure, 410, 444
Königsberg bridges problem, 194
Kuratowski's theorem, 202

Labeled graph, 196
digraph, 233
Lagrange Theorem, 373
Language, 406, 425
regular, 407, 413
types of, 413
Last element, 446
Lattice, 451–453
$\text{lcm}(a, b)$ (least common multiple), 323
Least common multiple, 323
Length:
of a path, 193, 235
of a vector, 103
of a word, 405
Level, 60, 236
Lexicographical order, 238, 444

Linear:
  equations, 107, 115
  order, 443
  search, 64, 66
Linear bounded automata, 415
Linearly ordered, 443
Linked list, 188
List, 57
  linked, 188
Literal, 481
LNR traversal, 282
Logarithmic functions, 56
Logic, 78–92, 486
  circuits, 486
  gates, 486
Logical:
  equivalence, 83
  implication, 87
  operations, 79
Loop, 191, 234
Lower bound, 447
LRN traversal, 282

Machine:
  finite state, 416
  Turing, 419, 431
Map, 201
  dual, 204
MAP $(\cdot)$, 372
Mapping of sets, 50, 372
Mathematical induction, 12
Matrices, 104–110
  determinant of, 110
  inverse of, 109
  multiplication, 106
  square, 108
Matrix, 104–110
  adjacency, 205, 239
  augmented, 108
  Boolean, 23
  path, 241
  reachability, 241
  of a relation, 30
Maximal:
  element, 446
  ideal, 402
  rectangle, 495
Maxterm, 513
Mean, 160, 176
Meet, 451
Member of a set, 1
Merge-sort, 66
Minimal:
  Boolean expressions, 483
  cover, 495
  element, 446
  path, 196
Minimal (*Cont.*):
  spanning tree, 199
Minterm, 483
Modular arithmetic, 55, 337
Monic polynomial, 378
Monoid, 367
Multigraph, 191
Multiplication of matrices, 106
Mutually exclusive events, 152

N (positive integers), 2, 315–318
$n(\cdot)$ (number of elements), 9
n-ary relation, 37
NAND gate, 489
Negation, 80
  of a quantifier, 90
Neighbor, 245
Next-state function, 408
NLR traversal, 282
Nodes, 188, 233, 276
  external, 279
  internal, 281
Nonplanar graph, 202
Nonsingular matrix, 109
NOR gate, 489
Norm, 103
Normal subgroup, 373
NOT gate, 487
Null set $\varnothing$, 2
  tree, 276
Number, cardinal, 61

One-to-one:
  correspondence, 53
  function, 52
Onto function, 53
Operations, 364
  set, 5, 13
OR gate, 486
Order, 315, 442
  in a Boolean algebra, 479
  dual, 442
  of an element, 374
  of a group, 371
  inequalities, 315
Ordered:
  pairs, 27
  partitions, 140, 145
  rooted tree, 237
  set, 442
Ordering, partial, 37, 442
Outdegree, 234

$P(n, r)$ (permutations), 136
Parallel arcs, 235
Parametric form, 127
Parent, 278, 294

Partially ordered set, 37, 442
Partition:
  ordered, 140
  of a positive integer, 445
  of a set, 11, 23, 36, 44
Pascal's triangle, 135
Path in a graph, 193, 235
  matrix, 241
  minimal, 196
  shortest, 196
  simple, 193
PERM (·), 372
Permutations, 136, 372
  with repetition, 137
PID (Principal Ideal Domain), 377
Pigeonhole principle, 139
Pivot, 114
Planar graphs, 200–203
  colorings, 203
Pointer, 188
Polish notation, 238
Polynomial, 378–382
  function, 52
  monic, 378
  roots of, 380
Poset (partially ordered set), 37, 442
Positive integers N, 2, 315–318
Postfix form, 238
Postorder traversal, 282
Power set, 10, 18
Precedes, 442
Prefix form, 238
Premises, 85
Preorder traversal, 282
Prime implicant, 402, 484
Prime number, 320
Principal ideal, 377
Priority queue, 190, 286
Probability, 152–162
  conditional, 155
Product:
  direct, 401
  fundamental, 481
  order, 444
  rule, 133
  set, 27
Production in a grammar, 412
Proper subset, 3
Proposition, 78–82
  truth table of, 80
Propositional:
  calculus, 78–85
  function, 87
Pruning algorithm, 253
Pumping Lemma, 411
Pushdown automata, 415

Q (rational numbers), 2
Quantifiers, 87–92
  negation of, 90
Quasi-order, 443
Queue, 190
  priority, 190, 286
Quintuple (Turing machine), 420
Quotient
  group, 373
  semigroup, 368
  set, 36

R (real number system), 2, 316
Random variable, 159–162
Range:
  of a function, 50
  of a relation, 28
Rate of growth, 65
Reachable vertex, 235
  matrix, 241
Real:
  line **R**, 316
  number system **R**, 2
Recognition of words, 409
Recursively defined functions, 59, 72
Reduced residue system, 328
Reflexive relation, 32
Region of a map, 201
Regular:
  expression, 407
  grammar, 414
  graph, 197
  language, 407
Relation, 27–38
  closure of, 34
  congruence, 325
  equivalence, 35
  graph of, 29
  matrix of, 30
Relative:
  complement, 6
  frequency, 152
Relatively prime, 328
Remainder:
  function, 55
  Theorem, 380
Repeated trials, 157, 171
Ring, 376–378
  of polynomials, 378–382
Root:
  of a binary tree, 276
  of a polynomial, 380
  of a tree, 236
Rooted trees, 236
  ordered, 237
Row (of a matrix), 104
  canonical form, 113

Row (of a matrix) (*Cont.*):
  equivalence, 113
  operations, 112, 125
  reduction, 112

Sample space, 152
Scalar, 10, 379
  multiplication, 105
Schroeder-Bernstein Theorem, 62, 74
Search:
  binary, 66
  breadth-first, 247
  depth-first, 247
Search tree, binary, 284
Semigroup, 367
Sequences, 57
  Fibonacci, 60
Sets, 1–11
  algebra of, 7
  countable, 62
  finite, 9
  indexed, 57
  ordered, 442
  product, 27, 444
  quotient, 36
Short-lex order, 444
Shortest path, 196
  algorithm, 244
Similar:
  binary trees, 277
  ordered sets, 449
Similarity mapping, 449
Simple:
  graph, 191
  path, 193, 239
Sink, 234
Sort, topological, 251
Source, 234
Spanning tree, 199
Special sequences, 490
Square matrices, 108–112
Stack, 190
Standard deviation, 160
Star graph, 202
State, 408, 419
  diagram, 409, 416
  table, 416
Strings, 58
Strongly connected, 235
Subgroup, 372
  normal, 373
Subsemigroup, 368
Subset, 2
  proper, 3
Substitution, Principle of, 83
Subtree, 276
Subword, 405
Succeeds, 442
Success, 158
Successor, 233, 444
  list, 233
Sum rule, 133
Sum-of-products, 481
  complete, 483
Summation symbol Σ, 58
Supremum (sup), 447
Surjective function, 53
Syllogism, Law of, 86
Symmetric:
  difference, 7
  group, 371
  matrix, 121
  relation, 33
Synthetic division, 63

Tables, truth, 80, 490
Tape (Turing machine), 417
  expression, 419
Tautology, 82
Terminal in a grammar, 411
Terminal node, 276
Ternary relation, 37
Totally ordered set, 443
Trail, 193
  traversable, 195
Transfinite induction, 450
Transitive relation, 33
  closure of, 35
Transpose of a matrix, 108
Traversable:
  multigraph, 195
  trail, 195
Traversal of binary trees, 282
Tree, 198
  binary, 276
  derivation, 414
  diagram, 38
  general, 294
  ordered, 237
  rooted, 236
  spanning, 199
Triangular form, 113
Trivial graph, 191
Truth:
  tables, 80–82, 490
  values, 78
Turing machine, 413, 431
Types of grammars, 413

UFD (unique factorization domain), 379
Unilaterally connected, 235
Union of sets, 5
Unique factorization domain, 379

Unit:
in a Boolean algebra, 379
matrix I_n, 108
in a ring, 376
Unity (identity) element in a ring, 376
Universal:
address system, 237
quantifiers, 88
set U, 2
Upper bound, 453
Usual order, 442
Utility graph, 202

$V(G)$, 190
Valid arguments, 4
Variable, 50
in a grammar, 412
random, 159
Variance, 161
Vectors, 102–105
Venn diagram, 3
Vertex, 190, 233
file, 246
isolated, 191

Warshall's algorithm, 242
Weakly connected, 235
Weighted:
graph, 196
path length, 290
Welch-Powell algorithm, 203
Well-ordered set, 449
principle, 318
Word, 405
empty, 405
Worst case, 64

Yes (accepting) states, 408

Z (integers), 2, 315
$\mathbf{Z}_m$ (integers modulo m), 327
Zero:
divisor, 376
element, 477
matrix, 104
vector, 103